Technical Specification Group Services and System Aspects Meeting #25, Palm Springs, USA

TSGS#25(04)0525

Source: **TSG SA WG2**
Title: **CRs on 23.240 (GUP Stage 2)**
Agenda Item: **7.2.3**

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #25.

S2 doc #	Title	Spec	CR #	cat	Version in	Rel	WI	S2 meeting	Clauses affected
S2-042811	Addition of missing security aspects	23.240	024r1	F	6.4.0	6	GUP	S2 #41	2, 4.1.3, 4.1.4, 4.1.5

3GPP TSG-SA2 Meeting #41
Montreal, Canada, 16-20 August 2004

Tdoc ⌘S2-042811

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.240** **CR** **024** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	Addition of missing security aspects
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	GUP
Date:	⌘	16/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one 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 one of the following releases:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	3GPP SA3 has analyzed the security aspects of GUP. SA3 has concluded that they would neither produce a new specification nor update one of the existing SA3 specifications for this purpose. They find that missing security aspects of GUP would be sufficiently covered by referencing the relevant Liberty specifications in the GUP Stage 2 and Stage 3 specifications.
Summary of change:	⌘	Liberty ID-WSF Security and Privacy Overview and Liberty ID-WSF Security Mechanisms have been added in the references. A reference to these specifications has been added in subclauses on ëAuthentication of profile accessí, ëAuthorization of profile accessí and ëPrivacy controlí.
Consequences if not approved:	⌘	Security aspects of GUP remain unspecified in detail.

Clauses affected:	⌘	2, 4.1.3, 4.1.4, 4.1.5			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	29.240
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	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.

First modified section

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 22.240: "Stage 1 Service Requirement for the 3GPP Generic User Profile (GUP)".

[2] Liberty Discovery Service Specification, http://www.projectliberty.org/

[3] Liberty ID-WSF SOAP Binding Specification, http://www.projectliberty.org/

[4] Liberty ID-WSF Data Services Template, http://www.projectliberty.org/

[5] Liberty ID-WSF Security and Privacy Overview, http://www.projectliberty.org/

[6] Liberty ID-WSF Security Mechanisms, http://www.projectliberty.org/

End of first modified section

Second modified section

4.1.3 Authentication of profile access

A GUP functionality exists that is responsible to authenticate applications. Authentication is a vital function to be passed before any kind of access to GUP data is granted. GUP shall adopt generic mechanisms such as used for the OSA framework approach. More specifically GUP shall use authentication mechanisms from Liberty Alliance Project as specified in Liberty ID-WSF Security and Privacy Overview [5] and Liberty ID-WSF Security Mechanisms [6].

4.1.4 Authorization of profile access

A GUP functionality exists that is responsible to authorise applications to access GUP data based on User specific or common privacy rules. All attempts to access the GUP data are to be authorized according to the defined policies which shall include the requestor information, the requested data, the target subscriber and the performed operation, or some of those.

GUP shall use authorization mechanisms from Liberty Alliance Project as specified in Liberty ID-WSF Security and Privacy Overview [5] and Liberty ID-WSF Security Mechanisms [6].

The GUP data structures need to satisfy the requirement to provide the authorization information on the different levels: profile, component or data element. In addition to the generic authorization data, additional service specific data may be defined (e.g. for LCS). The same applies for the authorization decision logic. The execution of the authorization logic leads to a decision whether a requestor is allowed to make the request at all, and additionally to which part of data the requestor has the appropriate access rights with regard to the nature of the request.

GUP provides mechanisms for the different GUP entities for managing the authorization data.

Both HPLMN based applications and non-HPLMN based applications are expected to send requests to the GUP Server. The GUP server shall have functionality to apply different authorization criteria, policy control and load control to HPLMN and non-HPLMN applications. Policy control and load control are out of the scope of the present document.

4.1.5 Privacy control

The tight connection of authentication, authorization and subscriber specific privacy requirements results in privacy control. Privacy control implies a centralized management for access rights including the subscriber's privacy requirements.

GUP shall use privacy control mechanisms and other privacy related features from Liberty Alliance Project as specified in Liberty ID-WSF Security and Privacy Overview [5] and Liberty ID-WSF Security Mechanisms [6].

End of modifications