Technical Specification Group Services and System Aspects Meeting #27, 14 - 17 March 2005,Tokyo, Japan **TSGS#27(05)0109**

Source: TSG SA WG2

Title: CR(s) to 23.240

Agenda item: 7.2.3

Document for: APPROVAL

S2 Tdoc	Title	Spec	CR	Rev	Cat	C_Ver	Rel	WI
S2-050276	Use of Discovery Service as Trusted Authority	23.240	026		F	6.6.0	Rel-6	GUP

3GPP TSG-WG SA2 Meeting #44
26th January – 2nd February 2005, Budapest, Hungary

Tdoc ⌘ S2-050276

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.240** **CR** **026** ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

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

Proposed change affects: | UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Use of Discovery Service as Trusted Authority
Source:	⌘	3GPP TSG_SA WG2
Work item code:	⌘	GUP
Date:	⌘	13/12/2004
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:	⌘	Use of Discovery service as a Trusted Authority is not yet defined.
Summary of change:	⌘	Clarify that the discovery service may be also used as a Trusted authority in the scope of GUP apart from its basic discovery functionality.
Consequences if not approved:	⌘	Support of basic security mechanism as requested by SA3 would be missing and cause misallignment with SA3 agreements on GUP security

Clauses affected:	⌘	4.1.3, 4.1.4 and 4.2.5

	Y	N		
Other specs affected: ⌘		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 CHANGE **********

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], Liberty Discovery Service [2] 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], Liberty Discovery Service [2] 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.

********** NEXT CHANGE **********

4.2.5 Applications

The applications that may apply GUP reference points Rg and Rp may be targeted for different purposes e.g. for value added services or subscription management. Both operator's own applications and third party applications are covered. The latter ones shall apply Rg reference point.

Additionally the applications may utilise a discovery service to discover the contact reference information if not found out by other means. A discovery service e.g., as specified in Liberty Discovery Service Specification [2], may also act as Trusted Authority providing essential security related information (e.g. preferences in terms of peer entity and message authentication mechanism to be used and authentication and/or authorization assertions). Different policies may be followed in the use of discovery service. It may be used by different applications in different ways: per each operation, occasionally or not at all. In general terms, ~~T~~third party applications belonging to external security domains ~~may~~ shall ~~need to~~ use a discovery service as a normal step, but in operator's services it may not be needed at all.

Applications have different authorization rights to the GUP data of different subscribers as agreed between the parties.

********** END **********