3GPP TSG SA WG3 Security — SA3#36 **S3-041035**
November 23-26, 2004
Shenzhen, China

3GPP TSG-SA WG2 meeting #43 **Tdoc S2-043841**
Seoul, Korea, 15-19 November 2004

Title:	Response LS on GUP Security Recommendations
Response to:	LS (S2-043429) on Reply LS on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements
Release:	Rel-6
Work Item:	GUP Security
Source:	SA2
To:	SA3
Cc:	CN4

Contact Person:
Name: Yunchao Hu
Tel. Number: +31 6 55303036
E-mail Address: yunchao.hu@ericsson.com

Attachments: -

1. Overall Description

SA2 thanks SA3 for the liaison related to GUP Security (S2-043429 / S3-040885) where SA2 was introduced to the role of Discovery Service as a Trusted Authority and where SA2 was asked about which component to use in the lack of a Discovery Service.

SA2 would like to note that currently the use of the Discovery Service in TS 23.240 is made optional in order for applications to get the contact reference information for the GUP Server if not known by other means. Considering the essential role of the Discovery Service also as a Trusted Authority, SA2 agrees that its use shall be further clarified at TS 23.240.

At the same time, and due to the wide range of applications and kind of deployments that could adhere to the GUP framework, SA2 does not believe that the support of the Discovery Service acting as a Trusted Authority should be mandated in all cases. For example, a GUP requestor over the Rg interface residing at the same security domain as the GUP Server might not require the support of a Discovery Service neither for being aware of the contact reference information of the GUP Server neither for being able to be authenticated and authorized for getting access to the requested profile information.

Following similar arguments, the support of the Discovery Service for the authentication of profile access requests in other scenarios where the security policy so may dictate shall be made mandatory (e.g. when the GUP requestor resides outside the security domain of the operator and/or when the GUP requestor resides at a UE)

In that way, SA2 has discussed the following changes to TS 23.240 that hopefully reflect SA3 needs in terms of the use of the LAP Discovery Service within the GUP Architecture.

********** 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 **********

2. Actions

To SA3

ACTION: SA2 kindly asks SA3 to review the proposed changes to TS [23.240] in relation to the support of the Discovery Service as a Trusted Authority and confirm whether these changes satisfy SA3 concerns.

3. Date of Next TSG-SA2 Meetings

SA2#44	26th January – 2nd February 2005	EU
SA2#45	4th – 8th April 2005,	China

4. References

[23.240] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2"

Liberty Alliance Specifications are publicly available at http://www.projectliberty.org/specs/index.html

- [LAP-WSF Security Mechanisms] http://www.projectliberty.org/specs/liberty-idwsf-security-mechanisms-v1.1.pdf
- [LAP ID-WSF Discovery Service] http://www.projectliberty.org/specs/liberty-idwsf-disco-svc-v1.1.pdf