3GPP TSG SA WG3 (Security) meeting #32 **S3-040035**

9-13 February 2004

Edinburgh, UK

Source: **Nokia, Ericsson**

Title: **GUP security directions follow-up**

Document for: **Discussion**

Agenda Item: **6.17**

Introduction

The present contribution is provided to capture the status of the Generic User Profile (GUP) work in 3GPP. The present document is an update of earlier submission S3-030581 at SA3#30.

Discussion

The GUP architecture is depicted in TS 23.240 as shown in figure (4.1) below.

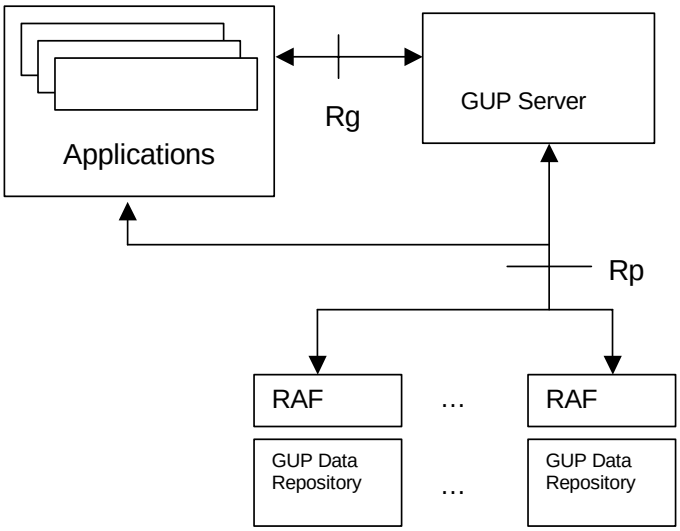

Figure 4.1: GUP reference architecture

There are two reference point Rg and Rp. TS 23.240 states:

Reference Points in the GUP Reference Architecture:

1. Reference point Rg
This reference point shall allow applications to create, read, modify and delete any user profile data using the harmonized access interface. The GUP Server locates the data repositories responsible of the storage of the requested profile component(s) and in case of proxy mode carries out the requested operation on the data. The reference point Rg shall support interworking to other mechanisms that support parts of the user profile outside the scope of 3GPP e.g. the Liberty Identity Web Services Framework Primer [3] and Liberty ID-WSF Data Service Template [4].
In the redirect mode, the GUP Server returns the locations of the GUP Data Repositories and the application can then send the requested operations via reference point Rp directly to the corresponding GUP Data Repositories.
The reference point Rg carries user related data, and therefore shall be protected by security mechanisms.

2. Reference point Rp
This reference point shall allow the GUP Server or applications, excluding third party applications, to create, read,

modify and delete user profile data using the harmonized access interface. Third party applications and third party GUP data repositories shall be connected to the GUP Server only using the Rg reference point.
The reference point Rp carries user related data, and therefore shall be protected by security mechanisms.

Note that the reference [3] above has been renamed and it has been proposed to be replaced by Liberty ID-WSF SOAP Binding Specification. The SA2 decision on this is pending. CN4 has made a decision to apply SOAP protocol in both Rp and Rg.

TS 22.240 defines requirements for GUP security and also TS 23.240 makes a few additional statements. See the annexes A and B of this contribution for more information.

The main tasks in the security area are:

- Authentication of applications and servers
- Integrity and confidentiality protection of messages
- Authorisation

The Liberty Identity Web Services Framework (ID-WSF) and ID Personal Profile have very similar tasks as GUP and SOAP is also applied in both. GUP Rg reference point may be seen as one Liberty ID Service Interface Specification. Note that ID-PP is not proposed as a part of GUP but it is mentioned here as a guiding example how profile services are defined according to Liberty ID-WSF. Thus we are proposing to specify GUP in alignment with Liberty ID-WSF.

The key security specifications of Liberty ID-WSF are:

- Liberty ID-WSF Security & Privacy Overview
- Liberty ID-WSF Security Mechanisms

Those specifications e.g. show how TLS/SSL can be used. Additionally message layer methods are provided taking advantage of X.509 or SAML (specified by OASIS) tokens. One issue to consider for GUP is whether the Rp reference point may have more simple security solutions than Rg which is the one used by third parties (see TS 23.240 text above). Regarding UE applications it is worth noting that a relationship to the Generic Authentication Architecture (GAA) work of SA3 exists.

Note: These Liberty ID-WSF specifications are approved and publicly available, together with the rest of Liberty specifications, at http://www.projectliberty.org/specs/index.html

Work status

The SA2#37 discussed a CR (S2-040267) about stating that the Rg reference point would be defined in compliance with the Liberty ID-WSF. SA2 was not able to make a decision yet, but delayed the issue further to the next co-located CN4 and SA2 meetings 16th – 20th February. We hope that a positive decision is taken and that the GUP Security could be based on the foundation laid by Liberty ID-WSF.
CN4 did little progress in their October meeting. The general principles and Liberty alignment were discussed and many documents postponed. T2 has continued working on Data Description Method (DDM) TS 23.241 which was sent for information to T plenary in December.

Proposal

It is seen that TLS with server and client side certificates makes a good basis for the security solution for GUP. Additionally the message layer security solutions of Liberty Alliance Project could be considered. We suggest that SA3 would consider taking the Liberty Alliance Project ID-WSF security solutions as the basis for the work. Furthermore, it is proposed to send a LS to SA2 and CN4 to provide SA3 view on adopting the Liberty ID-WSF for GUP security.

Annex A: Excerpt from Service requirement for the 3GPP Generic User Profile (GUP) TS 22.240 v.6.2.0:

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

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

3. It is permissible for either the supplier or consumer 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 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 of data to detect whether the data have been tampered with during transmission. .

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

8. It shall be possible for the supplier and/or the consumer 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.

8 Privacy and Authorisation

This clause describes the requirements for the authorisation of access to the user profile data. The Privacy can be provided by the means of authorisation mechanism.

8.1 General Requirements

It shall be possible for the user to define privacy requirements for components of the 3GPP Generic User Profile to determine access rights.
It is agreed in the subscription agreement between the home network operator and the subscriber how the access and privacy control is carried out e.g. who is able to control different parts of the user profile including the privacy settings.
The GUP shall provide means to implement access and privacy control according to the different agreements.
The GUP authorization shall be independent of who has set the privacy rules for each part of the GUP data. A generic mechanism shall be provided to ensure that only such data for which there is a valid authority can be created, read, modified or deleted.
The privacy requirements shall fulfill local privacy regulations. Lawful interception and other regulator requirements may imply that GUP data is delivered to authorities despite the privacy settings.

8.2 Authorisation Rules

Authorisation of the requested action (create, read, modify or delete) on the user profile data depends on the following information:

- identification of the requesting application
- identification of the requesting subscriber (if delivered in the request)
- identification of the targeted user
- identification of the targeted user profile data

The disclosure of the user profile data must be considered based on the identification of the application requesting access to the data. The possible identities of the applications will not be standardised but are implementation specific. Regarding trusted applications involving other subscribers or comparable entities it shall be possible also to check the access rights of the subscriber being served by the application. This requires that the identification of the served subscriber is passed via the GUP mechanism in addition to the application identification. The access is first defined per applications and secondly per served subscriber. The access may be granted also to the public, some group or a list of subscribers.

The identity of targeted user will be based on the 3GPP network identities (Private and Public User Identities). Public User Identities would be normally applied, but especially within the operator domain the Private Identity could be used as well.

The targeted user profile data will be controlled as per the whole user profile and/or per different GUP components and/or per different GUP data elements.

Depending on the service the privacy of the requested GUP data can additionally be managed in the service level e.g. in Presence or IMS group management. The privacy rules for these services are specified in the corresponding 3GPP specifications.

The GUP shall also support the possibility that the privacy of specific GUP data is queried from other privacy control system. Existing privacy solutions should be considered and adopted if applicable (e.g. LCS).

Annex B: Excerpts from 3GPP Generic User Profile - architecture TS 23.240 v.6.2.0:

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.

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 privacy rules. All attempts to access the GUP data are to be authorized according to the defined policies which shall include the requestor's identity.
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. How the generic decision logic is defined and provided is FFS.
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.

4.2.1.3 Authentication of profile request

The GUP Server shall make sure that the application requesting user profile data is properly authenticated. The authentication is based on the identification of the requesting application and/or the identification of the possible subscriber requesting the user profile data. The GUP Server may rely on the authentication made by other trusted entities.

4.2.1.4 Authorization of profile request

The GUP Server shall take care of the authorization of the access to the user profile data. The authorization itself may be handled by a separate entity in the network, or alternatively by the RAF or GUP Data Repository. The authorization shall be based on the requestor information, the requested data, the target subscriber and the performed operation, or some of them. The authorization rules of the requested data shall be defined at least in the GUP Component level in GUP Server. (Note that the authorization may be based on also on finer granularity of the data content.)