3GPP TSG SA WG3 Security — S3#29 **S3-030424**
15 - 18 July 2003
San Francisco, USA

3GPP TSG-SA WG2 Meeting #33 **Tdoc S2-032679**
Sophia Antipolis, France, 7th–11th July 2003

Title:	LS on usage of GUP reference points
Response to:	LS (S5-032227r5/S2-032117) on usage of GUP reference points from SA5
Release:	Release 6
Work Item:	3GPP Generic User Profile, Subscription Management
Source:	SA2
To:	SA5, SA3
Cc:	CN4, SA1, T2

Contact Person:
Name: Harri Koskinen
Tel. Number: +358 40 504 0780
E-mail Address: harri.o.koskinen@nokia.com

Attachments: none

---

1. Overall Description:

This LS is sent to SA3 for ACTION, and to SA5, CN4, SA1 and T2 for information.

SA2 would like to thank SA5 on their LS on usage of GUP reference points.

Concerning SA5's assumption on available documents for GUP, SA2 would like to point out that TS 23.240 has now been approved by SA #20 and raised to version 6.0.0.

SA2 would like to respond on SA5's questions as follows:

***Question A**: What is the relationship between the functional entities defined in 23.240 and those in 23.002?*

Answer: Figure 4.2 of TS 23.240 shows an example mapping the GUP reference architecture defined in Figure 4.1 to the current infrastructure environment. The GUP reference architecture does not specify or limit the physical location of the GUP Server enabling flexibility in the implementations.

***Question B**: What reference point is used to administer the security functions in the GUP server?*

Answer: Security functions are outside of the scope of SA2, they are specified by SA3.

***Question C**: GUP has the notion of a master GUP component. How is this master component allocated/defined?*

Answer: According to TS 22.240 the master component instance is responsible for the correct value of the corresponding GUP component. TS 23.240 specifies that the GUP Data Repository holds the master copy of the GUP component data. Applications or the GUP Server may copy (i.e. read) the component data or request synchronization. The master GUP component is created after the operation Create.

***Question D**: It is inevitable that at some point a computing or storage device will fail beyond recovery. What mechanisms exist for storage of data in alternative backup devices e.g. the ability to change the role of a non-master component to a master role. Also demote a master component to non-master?*

Answer: SA2 have not studied the reliability and backup issues of GUP Data Repositories, since the 3GPP Generic User Profile concept does not introduce any new network elements or new user related data. The objective of specifying the 3GPP Generic User Profile is to provide a conceptual description to enable harmonised usage of the user-related information located in different entities.

Changing the role of a non-master component to a master role is not possible, since after the change an Application would turn into a GUP Data Repository, and that is not allowed by the Rg and Rp reference points. Please see also the answer to Question C.

***Question E**: The GUP architecture shows usage of both the Rp and Rg reference points by applications. How does an application obtain an awareness of how data is distributed amongst the network, and hence which components support the RAF, to determine which components need to be communicated with via the Rp interface?*

Answer: Applications do not need to know how data is distributed amongst the network. The GUP Server provides a single point of access to the Generic User Profile data of a particular subscriber. The GUP Server supports two modes of operation. In both modes of operation the Application sends a request to the GUP Server.

In the proxy mode of operation the GUP Server makes requests to the GUP Data Repositories, receives responses from them and composes a response to the Application. The Application gets a response to its request from the GUP Server.

In the redirect mode of operation the GUP Server returns to the Application the information (e.g. address of GUP Data Repository(s)) to allow the Application to request the information from the GUP Data Repositories. The Application then directly requests the information from the GUP Data Repositories. Note also that third party applications are excluded from using the redirect mode of operation.

For more detailed information on this subject, please see subclause 4.2.1 of TS 23.240.

***Question F**: Are there any security mechanisms supported when using the Rp interface when accessing the RAF?*

Answer: Authorisation and authentication are required in TS 22.240 and TS 23.240. Additionally TS 23.240 states that since the reference point Rp carries user related data, it shall be protected by security mechanisms. Security mechanisms are outside of the scope of SA2, they are specified by SA3.

***Question G**: Subscription management in release 6 is aimed at being within the same network. With a future need after release 6 to support 3rd part operators and VASPs. Will GUP permit varying levels of access capabilities / restrictions to be defined for different Subscription management requestors?*

Answer: Yes. Both HPLMN based applications and non-HPLMN based applications are expected to send requests to the GUP Server. The GUP Server has the functionality to apply different authorisation criteria, policy control and load control to HPLMN and non-HPLMN applications.

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 authorisation is based on the requestor information, the requested data, the target subscriber and the performed operation, or some of them. The authorisation rules of the requested data are defined at least in the GUP component level in the GUP Server.

***Question H**: Subscription management will have an initial need to be able to configure data for the GPRS / IMS applications. This necessitates being able to configure data in the HSS for specific users. E.g. the data in 23.008, 23.016, 23.060. Is there any schema definition work in progress for any of the data in these specifications?*

Answer: CN4 will specify the concrete network specific GUP components in GUP stage 3 network specification TS 29.240.

***Question I**: Figure 4.2 of TS 23.240 depicts an RAF associated with Management Servers. The term 'Management Servers' is unknown to SA5. Please provide its definition and the source document.*

Answer: 'Management Server' is a generic term meaning any type of server used for management purposes, some examples are given in the figure. There is no SA2 definition or a source document for it.

2. Actions:

To SA3 group.

ACTION: SA2 asks SA3 group to answer Question B: "What reference point is used to administer the security functions in the GUP server?" and to give more detailed information on Question F: "Are there any security mechanisms supported when using the Rp interface when accessing the RAF?"

To SA5, CN4, SA1 and T2 groups.

ACTION: None.

3. Dates of Next TSG-SA WG2 Meetings:

TSG-SA WG2 Meeting #34	18th – 22nd August 2003	Brussels, Belgium
TSG-SA WG2 Meeting #35	27th – 31st October 2003	Asia
TSG-SA WG2 Meeting #36	24th – 28th November 2003	Sophia Antipolis, France