3GPP TSG-SA2 #30 *Tdoc S2-031006*
Milan, Italy, 24th ~ 28th February, 2003 **revised S2-030906**

Title: **Liaison Statement on GUP Interworking with Device Management**
Release: **Release 6**
Work Item: **GUP**

Source: **SA2**
To: **OMA DM WG, SA5**
CC: **T2, SA3**

Contact Person:
Name: Qing Xuan
E-mail Address: qing.xuan@vodafone.co.uk

Attachments: 23.240 1.0.0

---

1. Overall Description

SA2 would like OMA DM WG/SA5 to consider about the relationship between GUP and Device management in detail. This liaison statement aims to increase the common understanding on the interworking between GUP and Device management.

In the current 32.802 v5.1.0 section 6.1.1.3, the UEM gateway is defined as "UE Managers use the UEM Gateway to provide transparent access to the UE client from various UE Managers. In this example, the UEM Gateway controls the access available to the UE Managers. It is assumed that the network operator will own the UEM Gateway". This makes the UEM gateway appear similar to the GUP server, however, the GUP server does not just provide a single access with authentication and authorisation in a secure manner for UEM but also it finds the right data repository for device managers (routing) via Rp interface.

From the definition of the UEM Gateway and GUP server above, in order to avoid the overlap between GUP and Device management, SA2 would like OMA DM WG/SA5 to reference current 23.240 (specially Annex A) for device management interworking with GUP.

2. Actions

TSG SA WG2 kindly asks OMA DM WG/SA5 to consider for Release 6 device management interworking with GUP as described above in ongoing work on GUP 23.240.

3. Date of Next TSG SA WG2

TSG SA WG2 #31	**7th – 11th April 2003**	**Seoul, Korea**
TSG SA WG2 #32	**12th – 16th May 2003**	**San Diego, USA**

3GPP TS 23.240 V1.0.0 (2003-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP Generic User Profile - Architecture;
Stage 2
(Release 6)

Keywords
<User, Profile, Architecture>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The fact of having several domains within the 3GPP mobile system (e.g. Circuit-Switched, Packet-Switched, IP Multimedia Subsystem) and access technologies (e.g. GERAN, UTRAN and WLAN) introduces a wide distribution of data associated with the user. Further, the new functions both in terminals and networks mean that the data related to users, services and user equipment will be increased greatly. This causes difficulties for users, subscribers, network operators and value added service providers to create, access and manage the user-related data located in different entities.

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. Technically the 3GPP Generic User Profile provides an architecture, data description and interface with mechanisms to handle the data.

1 Scope

The present document defines the stage 2 architecture description to the 3GPP Generic User Profile (GUP), which includes the elements necessary to realise the stage 1 requirements in 3GPP TS 22.240 [1].

The present document includes the GUP reference architecture with descriptions of functional entities, and their interfaces and procedures, as well as the high-level information model for the GUP data.

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)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document the following definitions apply:

3GPP Generic User Profile (GUP): The 3GPP Generic User Profile is the collection of user related data which affects the way in which an individual user experiences services and which may be accessed in a standardised manner as described in this specification.

GUP Component: A GUP component is logically an individual part of the Generic User Profile.

GUP Data Element: the indivisible unit of Generic User Profile information.

Data Description Method: A method describing how to define the data contained in the Generic User Profile.

3.2 Symbols

For the purposes of the present document the following symbols apply:

Rg	Reference Point between Applications and the GUP Server.
Rp	Reference Point between the GUP Server and GUP Data Repositories, and between Applications and GUP Data Repositories.

3.3 Abbreviations

For the purposes of the present document the following abbreviations apply:

CLB	Component Location Broker
GAP	GUP Access Point
GUP	3GPP Generic User Profile
PAAC	Profile Authorisation & Authentication Control
RAF	Repository Access Function

4 Reference Architecture

4.1 GUP Functionalities

4.1.1 Harmonised access interface

The GUP harmonized access interface is the interface which can be used by the GUP suppliers and GUP consumers to access, manage and transfer the profile data. This application layer interface is independent of the profile structure.

4.1.2 Single Point of Access

There exists for each Profile a single point of access, which knows the location of the various components of the Profile.

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 a generic mechanisms such as used for the OSA framework approach.

4.1.4 Authorisation 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 authorised according to the defined policies which shall include the requestor's identity.

The GUP data structures need to satisfy the requirement to provide the authorisation information on the different levels: profile, component or data element. In addition to the generic authorisation data, additional service specific data may be defined (e.g. for LCS). The same applies for the authorisation 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 authorisation 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, Authorisation and subscriber specific privacy requirements results in Privacy control. Privacy control implies a centralized management for access rights including the subscriber's privacy requirements.

Editor's note: results are expected from the investigation on the feasibility study considering "Generalised privacy capability" (WI agreed at SA#17).

4.1.6 Synchronisation of data storage

Editor's note: this issue is under further investigations. Either an application is notified and requests the modified GUP data or the data modification is pushed to the application.

4.1.7 Access of profile from visited network

Access to GUP from a visited network shall follow the single point of access principle.

4.1.8 Location of Profile Components

A GUP functionality exists that keeps information where GUP data are located.

Editor's note: Further details are expected.

4.1.9 Charging for Profile Access

The GUP Server shall be capable of providing charging information, e.g. to enable transaction/event based charging.

Some GUP Data Repositories may provide charging information, while other GUP Data Repositories do not provide charging information.

Mechanisms are needed to permit the GUP Server to know which GUP Data Repositories are (and are not) producing their own charging information. When the GUP Data Repository is capable of producing charging information, mechanisms are needed for the correlation of the charging information produced by GUP Server and GUP Data Repository.

NOTE: GUP Data Repositories within a UE are not expected to produce charging information.

The charging information may also be used for other event logging, customer care, privacy auditing, etc. functions.

4.2 GUP Functional Entities

The GUP reference architecture as shown in Figure 4.1 consists of:

- GUP Server;
- Repository Access Function (RAF);
- GUP Data Repositories;
- Rg and Rp reference points;
- Applications.

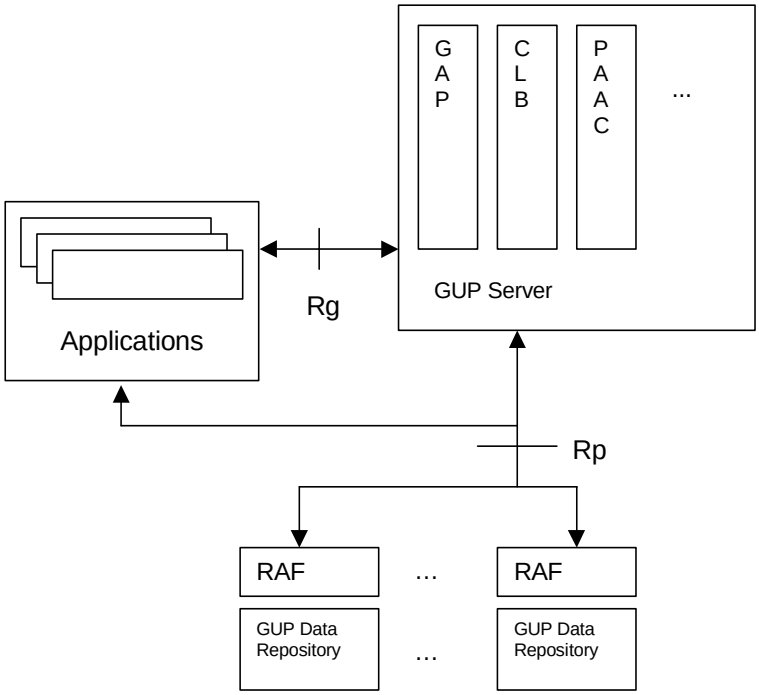

Figure 4.1: GUP Reference architecture

An example of mapping the GUP reference architecture to current infrastructure environment is shown in Figure 4.2.

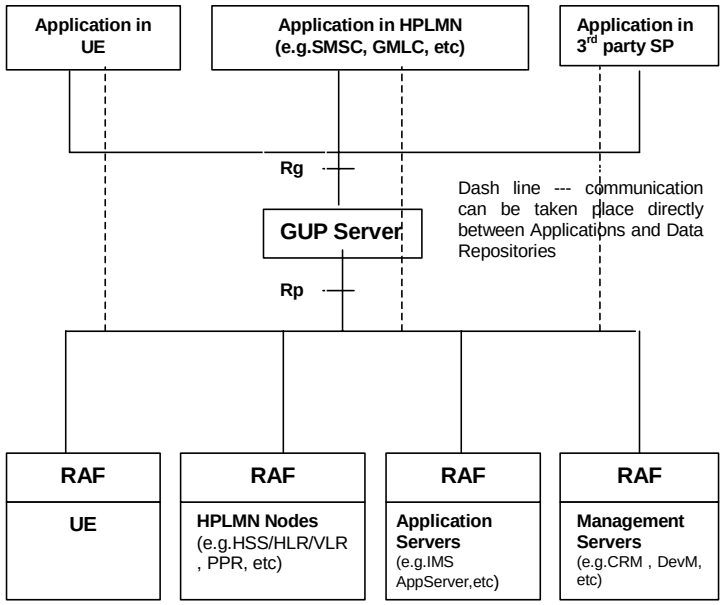

Figure 4.2: An example of mapping the GUP reference architecture to Current Infrastructure Environment

4.2.1 GUP Server

The GUP Server is a functional entity providing a single point of access to the Generic User Profile data of a particular subscriber. The Reference Architecture does not specify or limit the physical location of the GUP Server enabling flexibility in the implementations.

The GUP Server includes the following functionalities:

- To provide a single point of access for reading and managing generic user profile data of a particular subscriber.

Editor's note: Whether the GUP Server is implemented as a Proxy and/or Redirect Server must be defined later, see the two figures below.

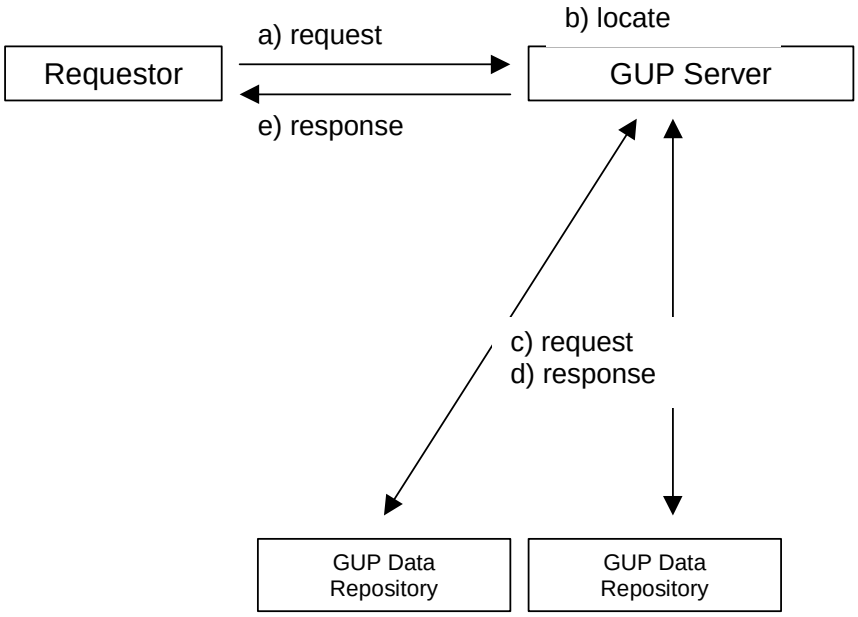

Figure 1. GUP Server acting as a Proxy Server.

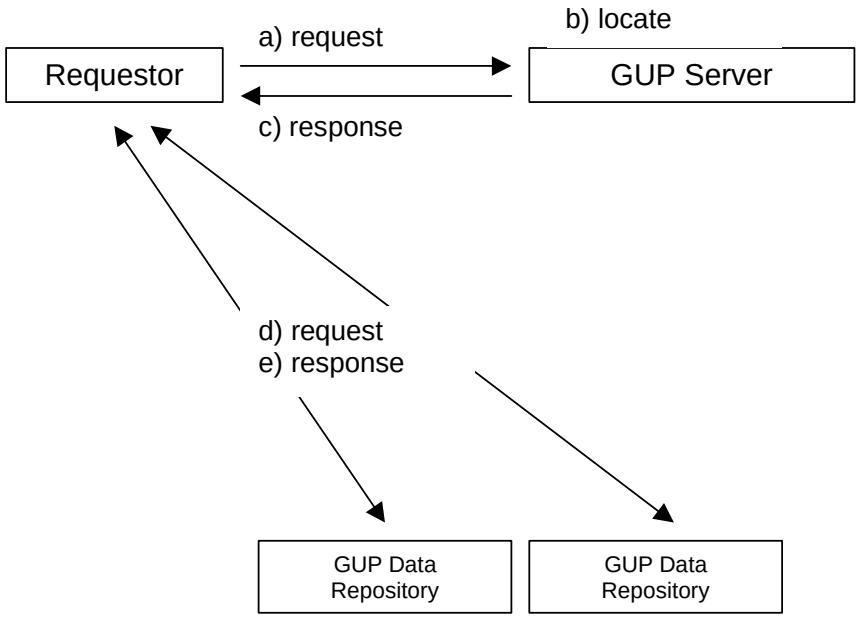

Figure 2. GUP Server acting as a Redirect Server.

Editor's note: How the functionality is performed to be added later.

Editor's note: Authentication, authorisation, privacy, synchronisation etc. to be added later.

4.2.2 Repository Access Function (RAF)

The Repository Access Function (RAF) realizes the Harmonised Access interface. It hides the implementation details of the data repositories from the GUP infrastructure. The RAF performs protocol and data transformation where needed.

The protocol between the RAF and the GUP data repository is out of the standardisation scope. It is recommended that the protocol used should support GUP requirements.

4.2.3 Reference Points

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 carries out the requested operation on the data.

Editor's note: The reference point Rg carries user related data, and therefore should 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.

Editor's note: The reference point Rp carries user related data, and therefore should be protected by security mechanisms.

4.2.4 Message Flow of using GUP

For an application requesting GUP data component(s) a message flow is described in the following:

- The application requests a GUP component(s) via Single Point of Access (Rg) from the component broker function at the GUP server
- The component broker function at the GUP server authenticates the application. Note that also separate authentication services may be applied.
- The component broker function at the GUP Server identifies the level of authorization the Application is allowed to access the GUP data.
- The component broker function at the GUP Server identifies the location of the GUP component(s).

At this point the Component Broker function at the GUP Server may (see figure 4.3 below)

- Access the GUP component(s) by means of the Harmonised Access Interface (Rp) or by other means outside the scope of GUP.
- Respond to the application with the result of the request, optionally combining results from different GUP data repositories.

Or, depending on GUP data repositories choice (see figure 4.4 below)

- Respond to the application with reference(s) to the component(s) and additionally authorisation credentials with limited lifetime. Note that authorisation credentials from other sources are not excluded.
- The application uses the reference(s) and the authorisation credentials to access GUP data repositories by means of the Rp reference point.

Privacy rules may stay together with the data it applies to at the data repository where the data is stored. In this case this privacy rules shall apply. Optionally, the GUP Server may apply additional privacy rules, handled at the PAAC function. However the GUP Server must never “bypass” existing privacy rules.

The following figures show the message flows for both cases as described.

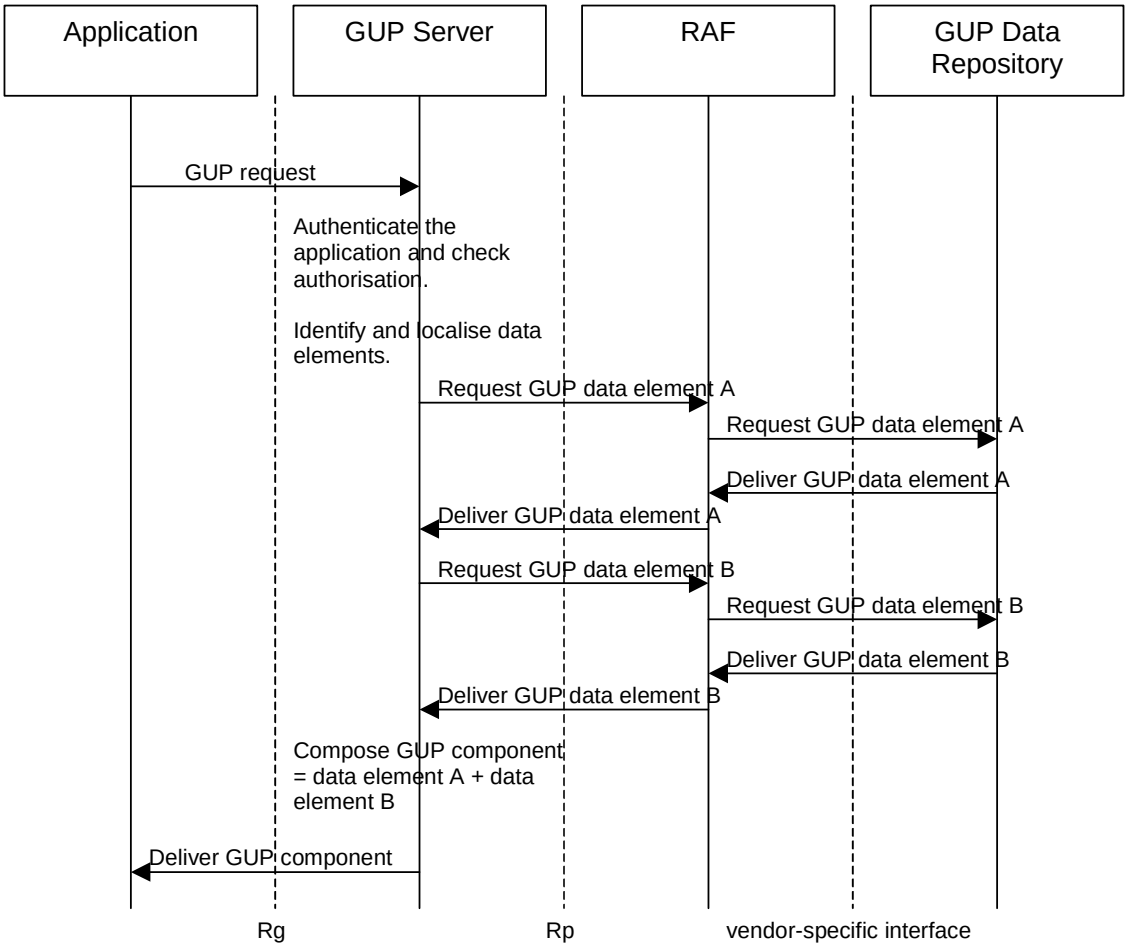

Figure 4.3: An Example of Application Requesting GUP Data Component(s) Message Flow

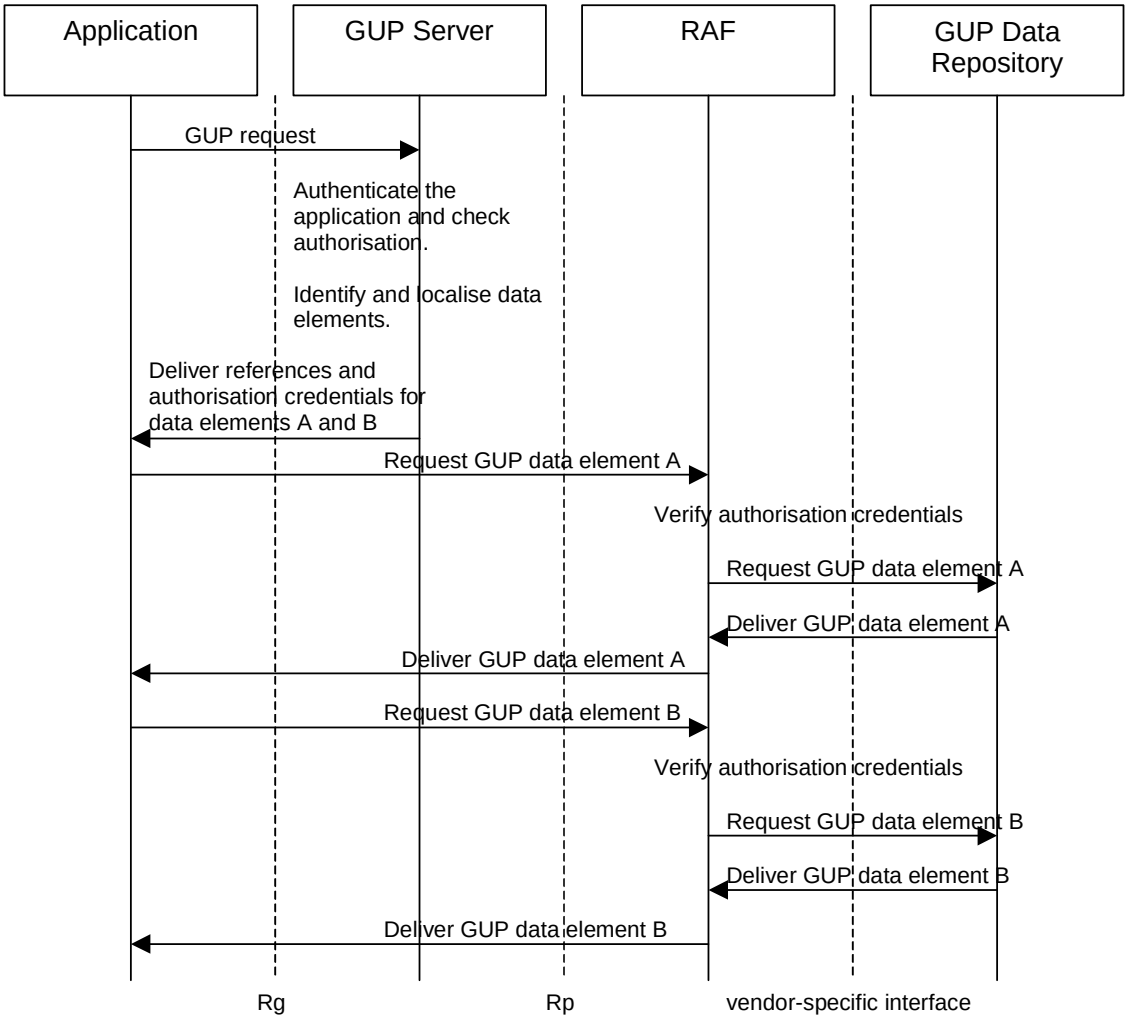

Figure 4.4: An Application Requesting GUP Data Component(s) Message Flow

4.3 Rp reference point procedures

This subclause defines the procedures applied in the Rp reference point. The application or GUP server acts as the active requestor towards the Repository Access Function (RAF) entities e.g. to read or modify the data. It is assumed that the both ends share initially the same data structure definitions. Rp is applied to control the data stored in the different user profile components as per users. To address the data the user identity or the component identification is given accompanied with the lower level data reference when required.

There are the following procedures:

- Create Component
- Delete Component
- Modify Data
- Read Data
- Subscribe To Data
- Notify Data
- Define Data

Editor's note: The input and output information elements are to be added to each procedure as well as the error type descriptions. The possible application authentication functions are also FFS.

Editor's note: How the existing profile components are included in the Generic User Profile is FFS.

4.3.1 Create Component procedure

Create Component procedure is used by the application to add a new profile component in the contacted repository. The attached user identity and the created component type are specified along with the created data. It is presumed that the profile data structure is already known by the both parties. No new type of data can be defined by this procedure, only the data contents are provided. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications). The RAF returns the component identification.

This procedure is synchronous in nature but it is also possible to define a separate response message.

4.3.2 Delete Component procedure

Delete Component procedure is used by the application to remove a profile component from the contacted repository. The attached user identity and the component type or the component identification is specified. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

4.3.3 Modify Data procedure

Modify Data procedure is used by the application to change the data in a profile component. The component is identified by the user identity and the component type or by the component identification. The modification may concern the whole component or any single lower level piece of data referenced in the procedure invocation. The new contents for the entire referenced data shall be provided. It is also possible to add more similar type of data elements to an existing array type of element. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

4.3.4 Read Data procedure

Read Data procedure is used by the application to retrieve the data in a profile component. The component is identified by the user identity and the component type or by the component identification. The data retrieval may concern the whole component or any single part of it as referenced in the invocation. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

4.3.5 Subscribe To Data procedure

Subscribe To Data procedure is used by the application to request notifications about changes in the profile component data. The component is identified by the user identity and the component type or by the component identification. Furthermore the application can identify which elements are to be monitored for changes if it is not interested in all changes. Data synchronisation can be performed by Subscribe To Data and Notify Data procedures. The RAF returns the identification of the subscription request to provide means for the application to link the notifications of Notify Data procedure to the related subscribe requests.

The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

4.3.6 Notify Data procedure

Notify Data procedure is invoked by the RAF when the data which was identified in Subscribe To Data procedure changes or alternatively when the notification is requested by management means outside the scope of this specification. The procedure identifies the changed data and optionally provides the new values.

4.3.7 Define Data procedure

Define Data procedure is used by the application to define new data elements to the profile component data structure. The names and types for the new data are specified. This procedure facilitates extension of the profile data with new, proprietary data. Subsequently these data can be handled by the above described procedures e.g. modifed by the Modify Data procedure.

4.3.8 Common information definitions

Editor's note: The information elements that are applied in several procedures are described in this chapter. Authorisation input data is one example.

4.3.9 Error handling and common error types

The basic principle in error handling is that all errors in carrying out the procedures lead to complete abortion of the requested operation. The procedure error responses identify the error type together with more detailed information about the cause of the error.

The common error types which can be applied to all procedures contain:

Table 4.1: Common error types

Error	**Description**
Invalid operation	The operation is invalid or unsupported.
Invalid parameter	The given parameter of the operation is invalid.
Unauthorised operation	There was no authority for the requested operation.
Data unavailable	The requested data were not available.
Unexpected error	An unexpected error condition was met.

5 GUP Information Model

A Generic User Profile consists of a number of independent Profile Components.

The Profile Component has a unique identity within the Generic User Profile.

A Profile Component contains zero or more Data Elements. A Composite Datatype is used to define which Data Elements belong to the Profile Component.

The UML Class Diagram below illustrates the basic concepts of the GUP Information Model.

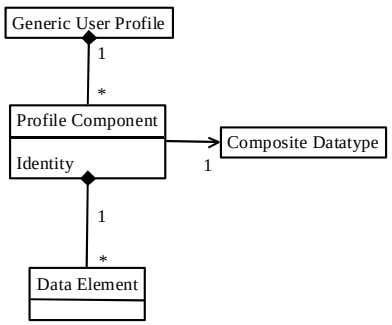

Figure 5.1: The basic concepts of GUP

Editor's note: The Information Model is a preliminary one: E.g. Logical/Physical view on Profile Component must be added later.

Annex A (informative): Examples of 3GPP Generic User Profile Usage

Example 1: GUP Interworking with Device Management

As the device management specification 32.802 requests, the UEM Gateway controls the access available to the UE managers. The GUP server will perform gateway functionality for device management. The example of the interworking interface diagram is shown in Figure A.1.

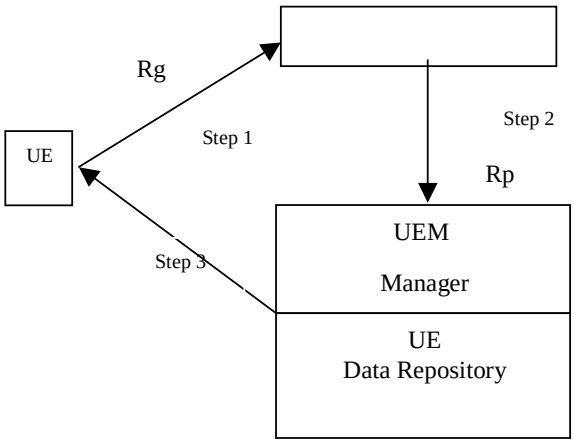

Figure A.1: An Example of the Interworking Diagram between GUP and Device Management

The interworking steps between GUP and Device management are summarised below:

Step 1: GUP Server allows any requests from UE to be accessed in a secured manner.

Step 2: GUP Server routes the request from UE to the appropriate UE management within the data repository.

Step 3: Data transactions take place.

Note: In this example the GUP server is working in proxy mode, this does not preclude the possibility for the GUP server to work in redirect mode when interworking with Device Management.

Annex B (informative): 3GPP Generic User Profile candidates

Editor's Note: Internal data accesses may be not considered as GUP accesses and in this case shall be deleted from this table.

This table lists the Generic User Profile candidates grouped per GUP access. It gives for each data access, the supplier, the consumer and the data repository. The applied categorisation of the data in the table does not imply similar GUP component structure.

GUP access	Supplier	Data repository	Description of the data	Consumer
Terminal related data for CS, PS, IMS	UE manager	UE-USIM/ISIM	Terminal capabilities of the terminal in use: - MS classmark 1, 2, 3 - User interface capability - Communication capabilities Data for initial configuration and/or reset of the ME Backup data for recovery of the ME Configuration including service specific data	UE MSC/VLR SGSN GGSN S-CSCF
General user data for CS & PS	UE manager	UE-USIM	USIM user data for CS&PS: - Language indicator - IMSI - Phone books - available services - service capabilities	UE-USIM MSC/VLR SGSN GGSN
General user data for IMS	UE manager AS manager	UE-USIM/ISIM AS	ISIM subscriber data for IMS: - Private & Public SIP URI of the user - Settings back up/restore - Preferences (e.g. languages) - Phone books - Buddy list - Available services - Service capabilities - Active service profile	UE-USIM/ISIM S-CSCF AS
MMS UE data Ref 31.102, 23.140	UE manager	UE-USIM	MMS notifications MMS issuer connectivity parameters MMS user preferences: - User preference profile name - Delivery report - Read reply - Sender visibility - Priority - Time of expiry - Earliest delivery time MMS connectivity parameters: - MMS server/server address - Case of WAP GW: Address Type of address Port Service Authentication type Authentication id. Authentication password - Case of core NW interface: Bearer Address Type of address Speed Call type Authentication type Authentication ID Authentication password	UE
MMS terminal capability negotiation Ref 31.102, 23.140	UE manager	MMS-UA	MMS terminal capability information: - maximum supported size of an MM - maximum supported resolution of an image - list of supported media types and media formats (e.g. MIME types) - list of supported character sets - list of preferred languages - maximum supported colour depth - indication whether or not the recipient MMS User Agent supports streaming for the retrieval of MM contents	MMS server
MMS VASP	AS manager	AS	MMS application specific data:	AS

applications Ref 23.141			- Authorization - Confidentiality - Charging information - Message distribution	MMS server
Privacy control settings of the user	AS manager	AS	Privacy control data of the user: - Privacy settings for standardised service like Presence - Privacy setting of non standardised services	UE-ISIM
PLMN specific user information	O&M	HSS	PLMN specific user information: - User addresses (e.g. MSISDNs, URLs) - WAP parameters (e.g. standard WAP gateway) - GPRS parameters - Preferred access technologies (e.g. UTRAN, GERAN, WLAN etc…)	S-CSCF AS
Authorised and subscribed service information for CS & PS	O&M HSS-HLR	HSS-HLR	Authorised and subscribed service information: - Subscriber ID (IMSI, MSISDNs) - General subscription information - Subscription restrictions - Basic & Supplementary services - Charging plans - Operator determined barring data is FFS - SMS subscription - MMS subscription	MSC/VLR GMSC SGSN GGSN MMS server
CSE handling of user subscriptions for CS & PS	CSE	HSS-HLR	- Forwarding & barring information - CAMEL subscription information	CSE
Authorised and subscribed service information for IMS	O&M	HSS	Authorised and subscribed service information: - IM Subscriber ID (Private User ID, Public ID) - Subscribed media - Billing policy - Initial filter criteria - Service keys & triggering aspects - Authorised services that the subscriber may subscribe to - Services the subscriber actually has subscribed to	HSS S-CSCF AS
CAMEL services for IMS	O&M	HSS-HLR	CAMEL subscription information for IMS	IM-SSF
MMS Ref 23.140	O&M	MMS server	MMS user subscription information: - information for the control of access to the MMS - information for the control of the extent of available service capability (e.g. server storage space) - a set of rules how to handle incoming messages and their delivery - information of the current capabilities of the users terminal	MMS server

Editor's Note: SMS is still missing from this table and will be added later.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
01-11-13		UP-010103			First version of the draft specification from UP-010065		
01-11-14		UP-010109			After UP#6 V0.2.0		
01-12-05		UP-010136			After UP#7 V0.3.0 Added changes from UP-010116 , UP-010134 and UP-010135 Reference added to GUP stage 1 TS 22.240 Chapter 8 moved under chapter 4 Chapter 10 moved to Annex A Editorial changes		
02-02-19		S2-020705			Outcome of SA2#23, version 0.4.0 with revision marks		
02-02-19		S2-020706			Outcome of SA2#23, version 0.4.1 clean copy		
02-06-25		S2-021881			Updates from SA2 drafting session		
02-06-25		S2-021882			Outcome of SA2#25, version 0.5.1 clean copy		
02-08-22		S2-022487			Outcome of SA2#26, version 0.6.0 with revision marks		
02-08-22		S2-022487			Outcome of SA2#26, version 0.6.1 clean copy		
02-10-15		S2-023067			Outcome of SA2#27, version 0.7.0 with revision marks		
02-10-15		S2-023067			Outcome of SA2#27, version 0.7.1 clean copy		
02-11-15		S2-023499			Outcome of SA2#28, version 0.8.0		
02-11-20		S2-023499r1			SA2#28 e-mail approval, version 0.9.0		
03-01-24		S2-030439			Outcome of SA2#29, version 0.10.0		
03-02-05		S2-030439r2			SA2#29 e-mail approval, version 0.11.0		
03-03-07		S2-030944			Produced for TSG-SA#19. Outcome of SA2#30 version 0.12.0.		