

ETSI TS 123 240 V17.0.0 (2022-04)



**Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP Generic User Profile (GUP);
Architecture (Stage 2)
(3GPP TS 23.240 version 17.0.0 Release 17)**



Reference

RTS/TSGS-0223240vh00

Keywords

LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations	6
3.1 Definitions	6
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Reference Architecture.....	7
4.1 GUP Functionalities	7
4.1.1 Harmonized access interface.....	7
4.1.2 Single point of access	7
4.1.3 Authentication of profile access.....	7
4.1.4 Authorization of profile access	7
4.1.5 Privacy control.....	8
4.1.6 Synchronization of data storage.....	8
4.1.7 Access of profile from visited network.....	8
4.1.8 Location of Profile Components	8
4.1.9 Charging for profile access	8
4.2 GUP functional entities	9
4.2.1 GUP Server	10
4.2.1.1 Single point of access	11
4.2.1.2 Location of profile components	12
4.2.1.3 Authentication of profile request.....	12
4.2.1.4 Authorization of profile request	12
4.2.1.5 Synchronization of profile components	12
4.2.1.6 Additional functionality	12
4.2.2 Repository Access Function (RAF)	12
4.2.3 GUP Data Repository	13
4.2.4 Reference Points	13
4.2.5 Applications.....	13
4.2.6 Message flow of using GUP	13
4.3 Rg reference point procedures.....	15
4.3.1 Create procedure.....	16
4.3.2 Delete procedure.....	17
4.3.2a List procedure	17
4.3.3 Modify procedure	18
4.3.4 Query procedure	19
4.3.5 Subscribe procedure.....	20
4.3.6 Unsubscribe procedure	21
4.3.7 Notify procedure.....	21
4.3.8 Common information definitions.....	22
4.3.8.1 Requestor data.....	22
4.3.8.2 Redirection data	22
4.3.9 Error handling and common error types	22
4.4 Rp reference point procedures.....	23
4.4.1 Create Component procedure	23
4.4.2 Delete Component procedure	24
4.4.2a List Data procedure.....	24
4.4.3 Modify Data procedure.....	25

4.4.4	Read Data procedure.....	26
4.4.5	Subscribe To Data procedure.....	26
4.4.6	Unsubscribe To Data procedure.....	27
4.4.7	Notify Data procedure	28
4.4.8	Define Data procedure	28
4.4.9	Common information definitions.....	28
4.4.9.1	Requestor data.....	28
4.4.10	Error handling and common error types	29
5	GUP information model	29
Annex A (informative):	Examples of 3GPP Generic User Profile usage.....	32
Annex B (informative):	3GPP Generic User Profile candidates	33
Annex C (informative):	Change history	34
History		35

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 harmonized 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 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)".
- [2] Liberty Discovery Service Specification, <http://www.projectliberty.org/>.
- [3] Liberty ID-WSF SOAP Binding Specification, <http://www.projectliberty.org/>.
- [4] Liberty ID-WSF Data Services Template, <http://www.projectliberty.org/>.
- [5] Liberty ID-WSF Security and Privacy Overview, <http://www.projectliberty.org/>.
- [6] Liberty ID-WSF Security Mechanisms, <http://www.projectliberty.org/>.
- [7] 3GPP TS 23.141: "Presence Service; Architecture and functional description".

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 standardized manner as described in this specification.

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

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

Data Element Group: A pre-defined set of Data Elements and/or other Data Element Groups closely related to each other. One or more Data Element Groups can constitute the GUP Component.

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:

FFS	For Further Study
GUP	3GPP Generic User Profile
HPLMN	Home PLMN
LCS	Location services
OSA	Open Service Access
PLMN	Public Land Mobile Network
RAF	Repository Access Function
UE	User Equipment
XML	eXtensible Markup Language

4 Reference Architecture

4.1 GUP Functionalities

4.1.1 Harmonized 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. A discovery service, e.g. Liberty Discovery Service Specification [2] may be used to get the contact reference information for this access point if not known by other means.

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] 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.

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.

GUP shall use privacy control mechanisms and other privacy related features from Liberty Alliance Project as specified in Liberty ID-WSF Security and Privacy Overview [5] and Liberty ID-WSF Security Mechanisms [6].

4.1.6 Synchronization of data storage

The GUP data repository holds the master copy of the GUP component data. Applications or GUP server may copy (i.e. read) the component data or request synchronization. The present document defines how the data is requested and sent. What is thereafter done with the data by the application or GUP server is beyond the scope of the present document.

Synchronization means that the changes to the master copy of the data are propagated to the entities that request synchronization. The synchronization request specifies which data are monitored for changes. It is also possible to request that all changes are reported.

Synchronization may cause heavy processing load to the involved entities, thus some policies are required in the implementations but those are not specified for the time being. However the GUP interfaces should carry sufficient data for enabling the load control mechanisms to work.

The entity under a heavy processing load has the responsibility to handle the error cases and conditions and to reach the synchronization as fast as possible. All the unresolved errors or load balancing actions that affect synchronization shall be reported.

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.

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.

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.

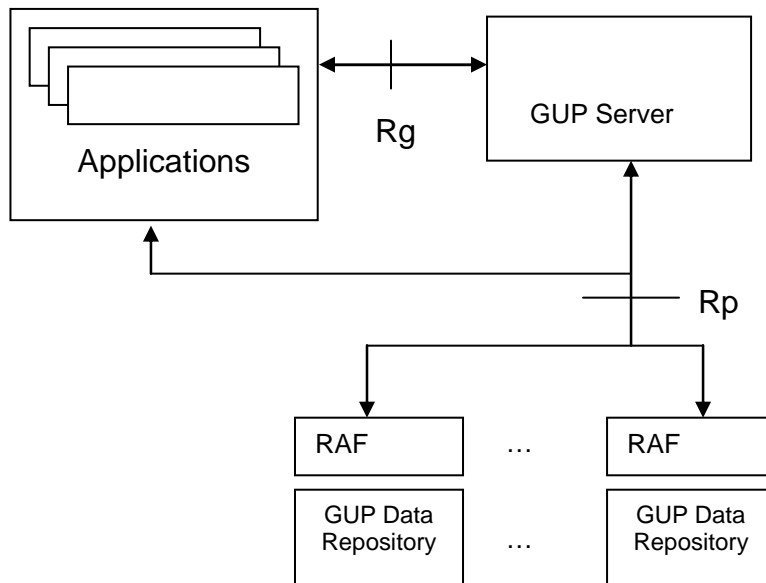


Figure 4.1: GUP reference architecture

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

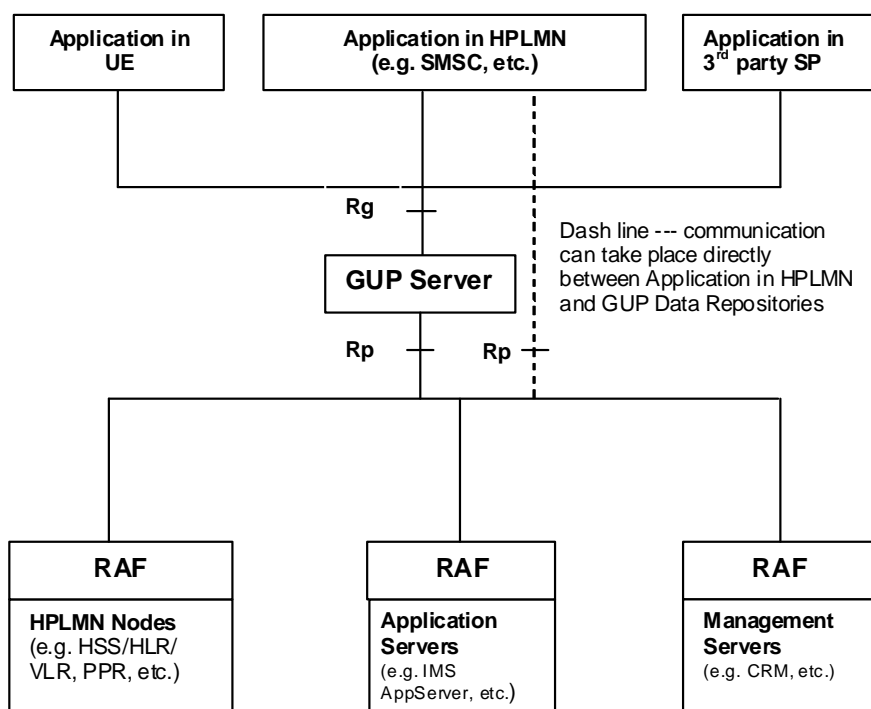


Figure 4.2: An example of mapping the GUP reference architecture to current infrastructure environment

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. However, the GUP Server shall be located in the home operator network of the targeted subscriber.

The GUP Server includes the following main functionalities:

- Single point of access for reading and managing generic user profile data of a particular subscriber.
- Location of Profile Components.
- Authentication of profile requests.
- Authorization of profile requests.
- Synchronization of Profile Components.

The GUP Server may support two modes of operation:

- **Proxy mode** (see figure 4.3). The Application requests user related data located in the GUP Data Repositories from the GUP Server. After taking care of needed actions specified for the GUP Server (and depending on the type of the request) the GUP Server makes requests to the corresponding GUP Data Repositories and receives responses from them. Finally the Application gets a response to the original request from the GUP Server. Depending on the type of the request also possible subsequent responses are delivered through the GUP Server.
- **Redirect mode** (see figure 4.4). The Application requests user related data located in the GUP Data Repositories from the GUP Server. After taking care of needed actions specified for the GUP Server (and depending on the type of the request) 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.

The Proxy mode is the default mode of operation. Redirect capability and preference for the applied mode may be indicated by the application with the Requestor data parameter when accessing the GUP Server. The GUP Server decides which mode is selected for the different requests. In addition to the Requestor data parameter, the decision is

based on the capabilities of the GUP Server and the related Repository Access Functions (RAF) as well as on the service configuration and policy data in the GUP Server related to the particular application. These service configuration and policy data are out of the scope of GUP standardisation. If the Redirect mode is not supported by the GUP Server the response is always sent according to the Proxy mode.

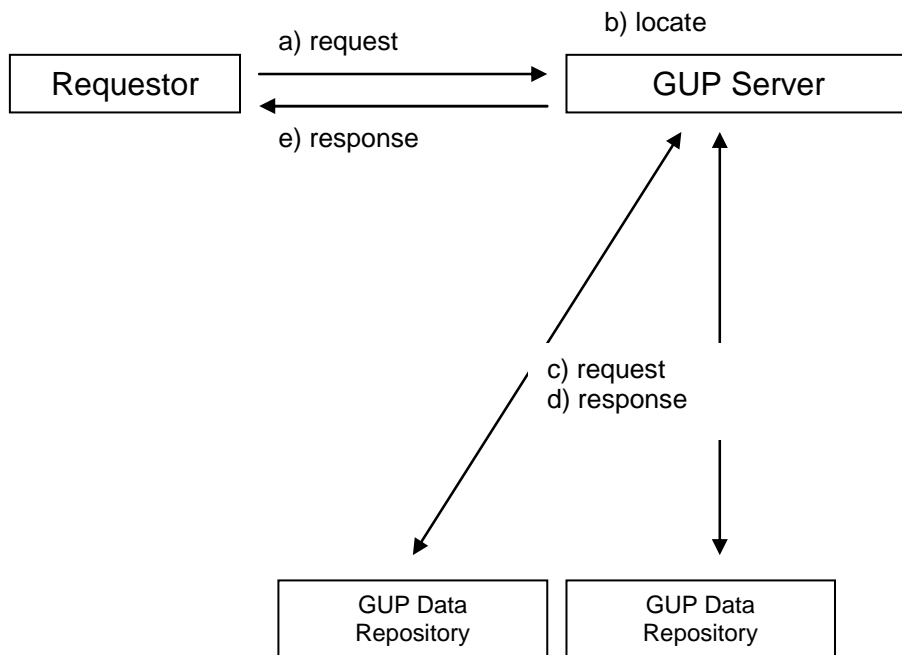


Figure 4.3: GUP Server acting as a Proxy Server

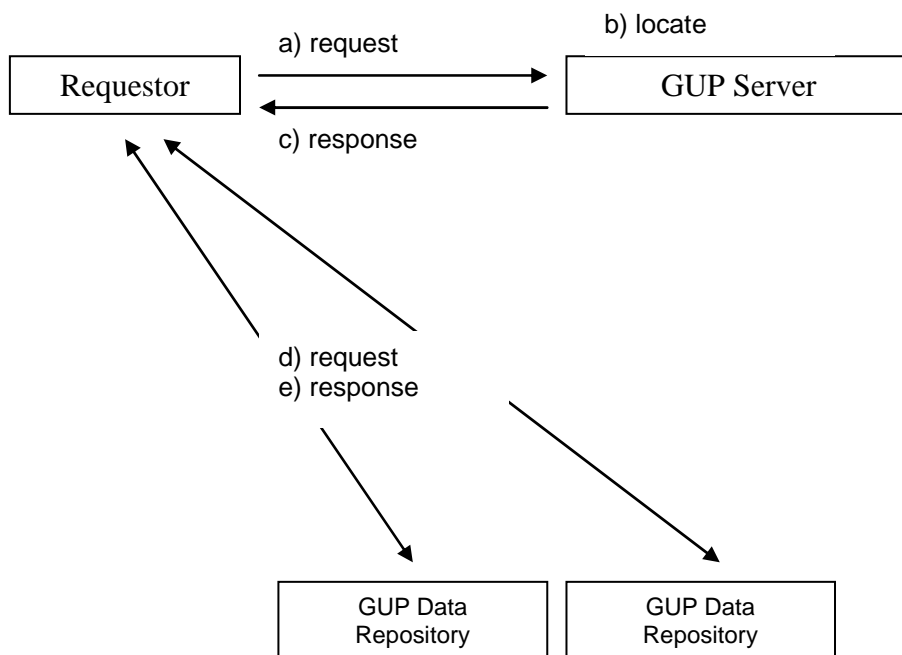


Figure 4.4: GUP Server acting as a Redirect Server.

4.2.1.1 Single point of access

The GUP Server shall accept data management related requests from the applications via the Rg reference point, and either convey the corresponding GUP component specific requests to GUP Data Repositories via Rp reference point or redirect the Application to convey the requests to the GUP Data Repositories. Note that one data request from an application to the GUP Server can cause sending of several GUP Data Repository requests by the GUP Server or Application. Also mapping to proprietary interfaces instead of Rp is possible in implementations.

In Proxy mode the GUP Server shall receive the results of the requests from GUP Data Repositories and deliver the results back to the requestor (Application). In case of responses from several GUP Data Repositories the GUP Server shall combine separate XML documents received from the repositories and deliver the composed information to the requestor. In redirect mode the Application will receive the results of the requests from the GUP Data Repositories.

4.2.1.2 Location of profile components

The GUP Server stores information about the GUP Components and the locations of data repositories of GUP Components related to each subscriber. Thus e.g. the separate GUP components composing the whole User Profile of a certain subscriber can be located and identified. The application shall be able to affect where a new GUP Component is created by the GUP Server. It is beyond this specification how the GUP server gets the component locations in the cases when it is not involved in the creation of those components.

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.) It shall be possible to manage the authorization data via the Rg and Rp reference points.

4.2.1.5 Synchronization of profile components

In proxy mode, the GUP Server shall convey the data synchronization requests from the applications to the RAFs in the same way as the other profile requests. Also the related change notifications from the RAFs are passed on to the requesting application. This requires that some kind of book keeping about the synchronization requests implemented. In redirect mode the GUP server shall redirect the Application to the RAFs in the same way as the other profile requests.

The GUP Server may store a copy of the actual data from the GUP Data Repository, but it is up to the local policy of the GUP Server.

4.2.1.6 Additional functionality

The GUP Server may take part in the charging of the data management operations concerning the profile.

The GUP Server may take part in the rate and/or size limiting of the data operations towards the profile.

The GUP Server may utilise a discovery service to register its contact reference information.

4.2.2 Repository Access Function (RAF)

The Repository Access Function (RAF) realizes the harmonized 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 standardization scope. It is recommended that the protocol used should support GUP requirements.

The RAF may take part in the authorization of access to such GUP information, which are under the control of the RAF. In addition, the authorization data may be managed via the Rp reference point.

4.2.3 GUP Data Repository

Each GUP Data Repository stores the primary master copy of one or several profile components. The RAF provides for the standardized access to the GUP Data Repository. The storage formats or the interface between the RAF and GUP Data Repository are not specified by GUP. It is presumed that the RAF and the GUP Data Repository are usually co-located in the same network element.

The GUP Data Repository may contain also the authorization data depending on the authorization model and architecture.

4.2.4 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 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. Liberty ID-WSF SOAP Binding Specification [3] and Liberty ID-WSF Data Services 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 external applications (e.g. located in a third party application or in the UE), to create, read, modify and delete user profile data using the harmonized access interface. Rp is an intra-operator reference point. External 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.

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, third party applications belonging to external security domains shall 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.

4.2.6 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 GUP server. The application will indicate if it can support the Redirect mode.
- The GUP server authenticates the application. Note that also separate authentication services may be applied.
- The GUP Server identifies the level of authorization the Application is allowed to access the GUP data.
- The GUP Server identifies the location of the GUP component(s).

At this point the GUP Server may (see figure 4.5 below)

- Access the GUP component(s) by means of the Harmonized 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 and if the application has indicated that it can support the Redirect mode (see figure 4.6 below)

- Respond to the application with reference(s) to the component(s) and additionally authorization credentials with limited lifetime. Note that authorization credentials from other sources are not excluded.
- The application uses the reference(s) and the authorization 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. However the GUP Server must never "bypass" existing privacy rules.

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

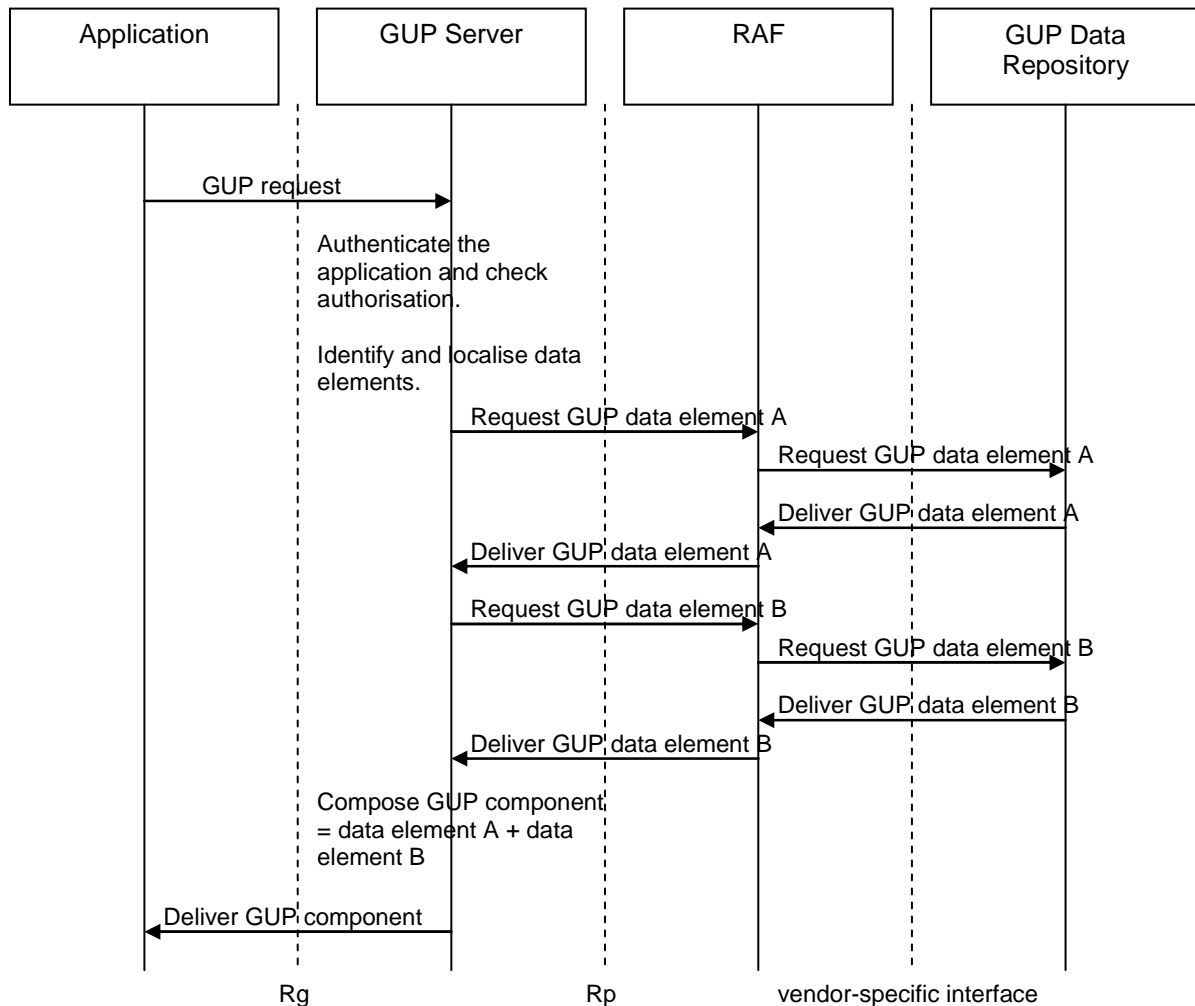


Figure 4.5: An Example of Application requesting GUP data component(s) message flow (Proxy mode)

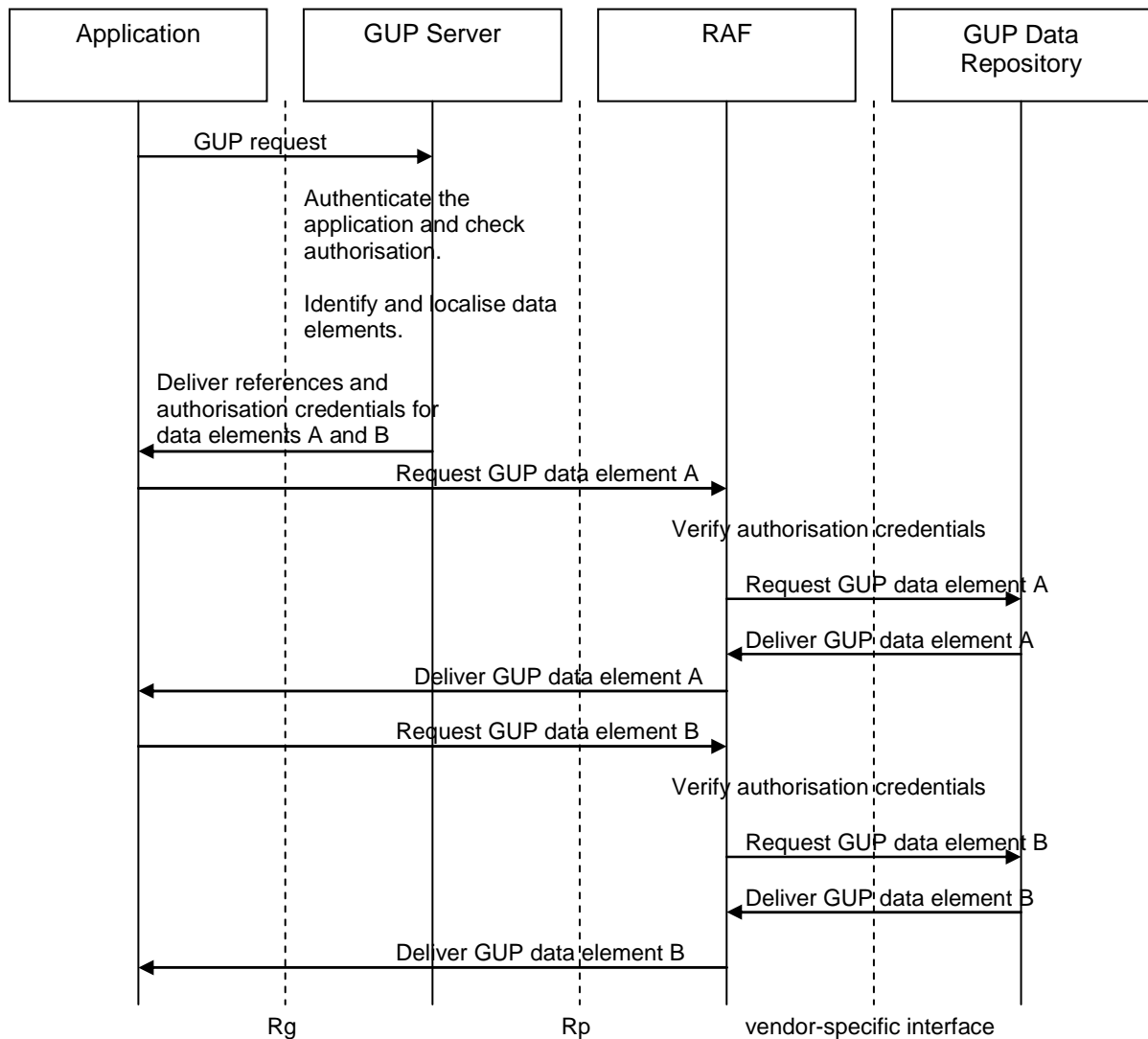


Figure 4.6: An Application requesting GUP data component(s) message flow (Redirect mode)

4.3 Rg reference point procedures

This clause defines the procedures applied in the Rg reference point between the applications and the GUP Server. This reference point supports also third party profile access. Rg can be used e.g. to create the whole user profile or some components in it, to read any piece of data in the profile or to modify those. There are means to authorise all requests and protect the user's privacy in all operations. Rg is applied to control the data stored in the different GUP components identified by a resource identity and the component type. The resource identity contains either a subscriber identity or a generic component identification, which is given to components that are not bound to a single subscriber.

There are the following procedures:

- Create
- Delete
- Modify
- List
- Query
- Subscribe
- Unsubscribe

- Notify

Instead of proxying the requests (or handling them by itself) the GUP Server may also apply the redirect mode of operation for applications that support redirect mode, which implies that the GUP Server responds to the request with the redirection information such as redirection address and authorisation assertions. Redirection can be made with Create, Delete, Modify, Query and Subscribe procedures.

4.3.1 Create procedure

Create procedure is used by the application to create a new user profile or new components to an existing profile. The procedure is always related to a single resource identity which is given in the request. Additionally the Create procedure shall carry the component types and the data to be created to each component. At least one component shall be provided. Creation of the first component implies profile creation. The component type identifies what data are concerned i.e. not just the data typing. 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. Furthermore the application shall provide the necessary data for authentication and authorization of this create function (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message. If the requestor data indicated that the application is able to receive redirect instructions, the GUP server may decide to return redirect instructions based on policies set by the operator in the GUP server. After this response the procedure is terminated without any other specified results or retained information in the GUP Server.

Table 4.1: Request data of Create procedure

Parameter	Description	Use
Resource Identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component data	Specifies which components are addressed and provides the data for those. There may be several Component data elements corresponding to several created components. At least one element must be present. See the table below for the more detailed contents.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.2: Contents of Component data parameter

Parameter	Description	Use
Component type	Specifies the type of the created component. The Component type identifies the applied component data definitions.	Mandatory
Data	Specifies the GUP component data according to the specified Component type.	Mandatory

Table 4.3: Response data of Create procedure

Parameter	Description	Use
Redirection data	Specifies the redirection instructions and assertions.	Optional
Status	Indicates whether: <ol style="list-style-type: none"> 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory (like the response itself)

4.3.2 Delete procedure

Delete procedure is used by the application to remove a profile or selected GUP components from the repository. The attached resource identity and the component type are specified. If no component type is provided, the whole user profile identified by the resource identity will be deleted. The application shall provide the necessary data for authentication and authorization purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message. If the requestor data indicated that the application is able to receive redirect instructions, the GUP server may decide to return redirect instructions based on policies set by the operator in the GUP server. After this response the procedure is terminated without any other specified results or retained information in the GUP Server.

Table 4.4: Request data of Delete procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component types	Specifies the types of the components.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.5: Response data of Delete procedure

Parameter	Description	Use
Redirection data	Specifies the redirection instructions and assertions.	Optional
Status	Indicates whether: 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory (like the response itself)

4.3.2a List procedure

List procedure is used by the application to list the existing profile items in the various GUP Data Repositories, and it is needed to handle large number of items. Different search criteria may be given as input. Only the references (i.e. resource identities and component types) are returned by the procedure. The listing may optionally operate sequentially, and then only a selected number of items is returned in one listing. The application shall provide the necessary data for authentication and authorization purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.5a: Request data of List procedure

Parameter	Description	Use
Search criteria	Specifies which profiles are to be listed. The criteria may include at least resource identity (or part of it) and/or component type.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.5b: Response data of List procedure

Parameter	Description	Use
Listing data	Provides the listed data (several elements). See the table below for the contents of a single element.	Mandatory
End indication	Indicates that the end of list has been reached.	Optional
Status	Indicates whether: 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory

Table 4.5c: Contents of Listing data parameter

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component types	Specifies the component types which are linked to the Resource identity and match with the search criteria.	Mandatory

4.3.3 Modify procedure

Modify procedure is used by the application to change the data in the GUP components. Also adding and deleting data is possible by Modify procedure, but it cannot create a new component. The modified data are identified by the resource identity and the data reference. The modification may concern the whole component or any lower level piece of data referenced in the procedure invocation. The contents for the entire referenced data shall be provided. Several individual changes to different components can be made with one procedure invocation. It must be noted that if modification of one component fails, the other changes cannot always be rolled back (implementation specific feature). However the response data shall specify which modifications were not accomplished. 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 authentication and authorization purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message. If the requestor data indicated that the application is able to receive redirect instructions, the GUP server may decide to return redirect instructions based on policies set by the operator in the GUP server. After this response the procedure is terminated without any other specified results or retained information in the GUP Server.

Table 4.6: Request data of Modify procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Modification data	Specifies which data are addressed and how those are changed. There may be several Modification data items corresponding to several individual modifications. These modifications may concern the same or different components. See the table below for the contents of one modification.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.7: Contents of Modification data parameter

Parameter	Description	Use
Data reference	Specifies which data are modified or expanded. The reference identifies both the component type and the possible deeper level data reference. The reference must be unique in a way that it refers only to one data item.	Mandatory
New data	Specifies the data to be stored in the GUP component. It is expected that all the data elements in the referenced data structure are given.	Mandatory
Overwrite indication	Specifies if the data are added to the existing data or replaces those. Default action is "insert".	Optional

Table 4.8: Response data of Modify procedure

Parameter	Description	Use
Redirection data	Specifies the redirection instructions and assertions.	Optional
Status	Indicates whether: <ul style="list-style-type: none"> 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory (like the response itself)

4.3.4 Query procedure

Query procedure is used by the application to retrieve the data in the user profile or its specific components. The queried data are identified by the resource identity and the data reference. The data retrieval may concern the whole profile, component or any parts of a component as referenced in the invocation. The requestor shall provide the necessary data for authentication and authorization purposes (e.g. credentials, assertions and identifications).

The retrieved data shall be provided in a separate response message. If the requestor data indicated that the application is able to receive redirect instructions, the GUP server may decide to return redirect instructions based on policies set by the operator in the GUP server. After this response the procedure is terminated without any other specified results or retained information in the GUP Server.

Table 4.9: Request data of Query procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Data references	Specifies which data are read. The data reference identifies the component type and the deeper level reference (if the whole component is not meant to be read). Multiple references may be given. It is also possible to refer to the profile root which implies that the whole profile data are queried.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.10: Response data of Query procedure

Parameter	Description	Use
Data	Contains the retrieved data as indicated by the Data references.	Mandatory
Redirection data	Specifies the redirection instructions and assertions.	Optional
Status	Indicates whether: 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory

4.3.5 Subscribe procedure

Subscribe procedure is used by the application to request notifications about changes in the GUP component data. The subscribed data are identified by the resource identity and the data reference. Furthermore the application can identify which elements are to be monitored for changes if it is not interested in all changes. Data synchronization can be performed by Subscribe and Notify procedures. The GUP Server returns the identification of the subscription request to provide means for the application to link the notifications of Notify procedure to the related subscribe requests. With Subscribe procedure an application can also request a list of all its subscriptions to notifications from the GUP Server. The GUP Server shall provide all the application's subscriptions to notifications in the response message.

A filtering data parameter is defined to facilitate performance optimization. This may be left partly vendor/operator specific. The requestor shall provide the necessary data for authentication and authorization purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message. If the requestor data indicated that the application is able to receive redirect instructions, the GUP server may decide to return redirect instructions based on policies set by the operator in the GUP server. After this response the procedure is terminated without any other specified results or retained information in the GUP Server.

Table 4.11: Request data of Subscribe procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID). This parameter may be absent only when List of subscriptions parameter is present, otherwise this parameter shall always be present.	Conditional
Notification Reference	Specifies the call-back address of the Requestor. The GUP server shall send the notifications to this address.	Mandatory
List of subscriptions	Indicates that the application requests the list of all its subscriptions from the GUP server.	Optional
Data references	Specifies which data are monitored for changes. The reference identifies both the component type and the possible deeper level data reference. Multiple references may be given. Any change within the referenced data structure causes a notification to be sent. If the parameter is absent, all modifications are notified.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional
Filter data	Specifies additional conditions for sending notifications to optimize the performance e.g. when immediate synchronization is not required. The parameter specifies also whether the initial data values are requested to be reported.	Optional

Table 4.12: Response data of Subscribe procedure

Parameter	Description	Use
Invoke identifications	Contains the invoke identification assigned by the GUP Server for this request. When the application has requested the list of all its subscriptions, this parameter will contain all the invoke identifications assigned by the GUP Server to the application.	Mandatory (unless the request is redirected or fails)
Redirection data	Specifies the redirection instructions and assertions.	Optional
Status	Indicates whether: 1. The procedure was carried out successfully, 2. The request was redirected, or 3. A failure was detected. For the proxy mode 1 or 3 can be indicated. For the redirect mode 2 or 3 can be indicated. The possible failure is described in sufficient detail.	Mandatory (like the response itself)

4.3.6 Unsubscribe procedure

Unsubscribe procedure is used by the application to cancel one or several existing subscriptions. The outcome of the procedure shall be provided in a separate response message.

Table 4.13: Request data of Unsubscribe procedure

Parameter	Description	Use
Invoke identifications	Specifies one or several invoke identifications assigned by the GUP Server for the subscriptions.	Mandatory

Table 4.14: Response data of Unsubscribe procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.7 Notify procedure

Notify procedure is invoked by the GUP Server when the data which was identified in Subscribe procedure changes or when the invoked Subscribe procedure requested sending of all the initial values of the referenced data. The procedure identifies the changed data and provides the new values.

The outcome of the procedure shall be provided in a separate response message.

Table 4.15: Request data of Notify procedure

Parameter	Description	Use
Invoke identification	Specifies the invoke identification assigned by the GUP Server for this subscription.	Mandatory
Notified data	Specifies which data are reported together with the data itself. Multiple pieces of data may be provided.	Mandatory

Table 4.16: Response data of Notify procedure (optional)

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (however the whole response is optional)

4.3.8 Common information definitions

The information elements that are applied in several procedures of Rg reference point are described in this clause.

4.3.8.1 Requestor data

The Requestor data contain the information that the sender of the request provides in order to facilitate the authentication and authorization functions. The access control and user privacy functions work based on these data. Also an unspecified Additional info parameter is defined to carry data e.g. for monitoring or accounting purposes. All the elements are optional. However at least one shall be present if the parameter is applied.

Table 4.17: Requestor data

Element	Description	Use
Subscriber identification	Specifies the end user being served.	Optional
Application identification	Specifies the application being served. The GUP Server has to link the Application identification to the actual sender of the request by the appropriate means taking into account the applied security measures and domains.	Optional
Credentials	Contains authentication information.	Optional
Authorization assertion	Contains the assertion for authorization. The nature of the assertion must be for one time use to prevent replay and cut-and-paste attacks. E.g. digest or signature mechanisms may be applied.	Optional
Privacy policy	Information about the applied privacy policy.	Optional
Redirection indications	Specifies if the application being served is able to handle returned redirect requests or if it specifically desires to apply the redirect mode. However the GUP Server decides which mode is used. If the parameter is missing, it is presumed that no such capability exists with the application.	Optional
Additional info	Additional unspecified information related to the requestor or request.	Optional

4.3.8.2 Redirection data

The Redirection data is returned to the requester if redirection is called for. These data contain the address where the request is to be redirected to and the authorisation assertions optionally provided by the GUP Server, which may this way carry out at least part of the authorisation on behalf of the RAF (or Data Repository). The RAF (or the GUP Data Repository) takes the final decision whether the authorisation is accepted or not.

Table 4.17a: Redirection data

Element	Description	Use
Redirection address	Specifies the address (e.g. URI) where the request is to be redirected.	Optional
Authorisation assertion	Contains the assertion for authorisation. This may be placed in the Requestor data item in the subsequent requests over Rp reference point.	Optional

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. However if e.g. multiple modifications with separate data references are made with one procedure invocation, it is possible that part of these are completed even if some would fail. 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 4.18: Common error types

Error	Description
Invalid operation	The operation is invalid or unsupported.
Invalid parameter	The given parameter of the operation is invalid.
Unauthorized 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.
Authentication error	The authentication of the requestor has failed.

4.4 Rp reference point procedures

This clause 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 identified by a resource identity and the component type. The resource identity contains either a subscriber identity or a generic component identification which is given to components that are not bound to a single subscriber.

There are the following procedures:

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

4.4.1 Create Component procedure

Create Component procedure is used by the application to add a new profile component in the contacted repository. The attached resource identity and the created component type are specified along with the created data. The component type identifies what data are concerned i.e. not just the data typing. 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 authorization purposes (e.g. assertions and identifications).

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

Table 4.19: Request data of Create Component procedure

Parameter	Description	Use
Resource Identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the created component. This is needed because several types may be supported by one RAF. The Component type identifies the applied component data definitions.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorization process. E.g. end user and application identification. See clause 4.4.9.	Optional
Component data	Specifies the profile component data according to the specified Component type.	Mandatory

Table 4.20: Response data of Create Component procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.2 Delete Component procedure

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

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

Table 4.21: Request data of Delete Component procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorization process. E.g. end user and application identification. See clause 4.4.9.	Optional

Table 4.22: Response data of Delete Component procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.2a List Data procedure

List Data procedure is used by the application to list the existing profile items in the various GUP Data Repositories, and it is needed to handle large number of items. Different search criteria may be given as input. Only the references (i.e. resource identities and component types) are returned by the procedure. The listing may optionally operate sequentially, and then only a selected number of items is returned in one listing. The application shall provide the necessary data for authentication and authorization purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.22a: Request data of List Data procedure

Parameter	Description	Use
Search criteria	Specifies which profiles are to be listed. The criteria may include at least resource identity (or part of it) and/or component type.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorization process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.22b: Response data of List Data procedure

Parameter	Description	Use
Listing data	Provides the listed data (several elements). See the table below for the contents of a single element.	Mandatory
End indication	Indicates that the end of list has been reached.	Optional
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory

Table 4.22c: Contents of Listing data parameter

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component types	Specifies the component types which are linked to the resource identity and match with the search criteria.	Mandatory

4.4.3 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 resource identity and the component type. The modification may concern the whole component or any lower level piece of data referenced in the procedure invocation. The contents for the entire referenced data shall be provided. Several individual changes to the component can be made with one procedure invocation. 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 authorization purposes (e.g. assertions and identifications).

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

Table 4.23: Request data of Modify Data procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Modified data	Specifies which data are addressed and how those are changed. There may be several modified data items corresponding to several individual modifications. See the table below for the contents of one modification.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorization process. E.g. end user and application identification. See clause 4.4.9.	Optional

Table 4.24: Contents of Modified data parameter

Parameter	Description	Use
Data reference	Specifies which data are modified or expanded. The reference may indicate the whole component or any deeper level piece of data. The reference must be unique in a way that it refers only to one data item.	Mandatory
New data	Specifies the data to be stored in the profile component. It is expected that all the data elements in the referenced data structure are given.	Mandatory
Overwrite indication	Specifies if the data are added to the existing data or replaces those. Default action is "insert".	Optional

Table 4.25: Response data of Modify Data procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.4 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 resource identity and the component type. The data retrieval may concern the whole component or any parts of it as referenced in the invocation. The requestor shall provide the necessary data for authorization purposes (e.g. assertions and identifications).

Table 4.26: Request data of Read Data procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Data references	Specifies which data are read. The data reference may point to a piece of data on any level in the data structure (also to the whole component). Multiple references may be given.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorization process. E.g. end user and application identification. See clause 4.4.9.	Optional

Table 4.27: Response data of Read Data procedure

Parameter	Description	Use
Data	Contains the retrieved data as indicated by the Data references. All the data under the referenced one are returned. Multiple packets of data are given if so requested.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

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

4.4.5 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 resource identity and the component type. Furthermore the application can identify which elements are to be monitored for changes if it is not interested in all changes. Data synchronization 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. With Subscribe To Data procedure an application can also request a list of all its subscriptions to notifications from the RAF. The RAF shall provide all the application's subscriptions to notifications in the response message.

A filtering data parameter is defined to facilitate performance optimization. This may be left partly vendor/operator specific. The requestor shall provide the necessary data for authorization purposes (e.g. assertions and identifications).

Table 4.28: Request data of Subscribe To Data procedure

Parameter	Description	Use
Resource identity	Specifies the resource identity with its type (e.g. SIP URI public ID). This parameter may be absent only when List of subscriptions parameter is present, otherwise this parameter shall always be present.	Conditional
Notification Reference	Specifies the call-back address of the Requestor. The RAF shall send the notifications to this address.	Mandatory
List of subscriptions	Indicates that the application requests the list of all its subscriptions from the RAF.	Optional
Component type	Specifies the type of the component.	Mandatory
Data references	Specifies which data are monitored for changes. Multiple references may be given. Any change within the referenced data structure causes a notification to be sent. If the parameter is absent, all modifications are notified.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorization process. E.g. end user and application identification. See clause 4.4.9.	Optional
Filter data	Specifies additional conditions for sending notifications to optimize the performance e.g. when immediate synchronization is not required. The parameter specifies also whether the initial data values are requested to be reported.	Optional

Table 4.29: Response data of Subscribe To Data procedure

Parameter	Description	Use
Invoke identifications	Contains the invoke identification assigned by the RAF for this request. When the application has requested the list of all its subscriptions, this parameter will contain all the invoke identifications assigned by the RAF to the application.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.6 Unsubscribe To Data procedure

Unsubscribe To Data procedure is used by the application to cancel one or several existing subscriptions.

Table 4.30: Request data of Unsubscribe To Data procedure

Parameter	Description	Use
Invoke identifications	Specifies one or several invoke identifications assigned by the RAF for the subscriptions.	Mandatory

Table 4.31: Response data of Unsubscribe To Data procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.7 Notify Data procedure

Notify Data procedure is invoked by the RAF when the data which was identified in Subscribe To Data procedure changes or when the invoked Subscribe To Data procedure requested sending of all the initial values of the referenced data. The procedure identifies the changed data and provides the new values.

Table 4.32: Request data of Notify Data procedure

Parameter	Description	Use
Invoke identification	Specifies the invoke identification assigned by the RAF for this subscription.	Mandatory
Notified data	Specifies which data are reported together with the data itself. Multiple pieces of data may be provided.	Mandatory

Table 4.33: Response data of Notify Data procedure (optional)

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (however the whole response is optional)

4.4.8 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. modified by the Modify Data procedure.

4.4.9 Common information definitions

The information elements that are applied in several procedures are described in this clause.

4.4.9.1 Requestor data

The Requestor data contain the information that the sender of the request provides in order to facilitate the authorization functions. The access control and user privacy functions work based on these data. Also an unspecified Additional info parameter is defined to carry data e.g. for monitoring or accounting purposes. All the elements are optional. However at least one shall be present if the parameter is applied.

Table 4.34: Requestor data

Element	Description	Use
Subscriber identification	Specifies the end user being served.	Optional
Application identification	Specifies the application being served. The RAF has to link the Application identification to the actual sender of the request by the appropriate means taking into account the applied security measures and domains.	Optional
Authorization assertion	Contains the assertion for authorization. The nature of the assertion must be for one time use to prevent replay and cut-and-paste attacks. E.g. digest or signature mechanisms may be applied. The provisioning of the assertions or any related shared secrets is beyond Rp reference point specifications.	Optional
Additional info	Additional unspecified information related to the requestor or request.	Optional

4.4.10 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 4.35: Common error types

Error	Description
Invalid operation	The operation is invalid or unsupported.
Invalid parameter	The given parameter of the operation is invalid.
Unauthorized 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.
Authentication error	The authentication of the requestor has failed.

5 GUP information model

A Generic User Profile consists of a number of independent GUP Components. However, a GUP Component may contain (i.e. reference) other GUP components e.g. to enable reuse of data.

The GUP Component has a unique identity within the Generic User Profile. In addition to the component type the component identity contains either a subscriber identity or more generic identification depending on which kind of component is in question. A GUP Component can be retrieved through one RAF, and it may consist of a number of GUP Components, Data Element Groups and/or Data Elements.

A GUP Component contains zero or more Data Element Groups. The Data Element Group contains indivisible Data Elements and/or Data Element Groups. The nested Data Elements Groups allow deeper hierarchical structures. The Data Element Group in the lowest hierarchical level contains one or more Data Elements. The Data Element Groups inside a GUP Component may be of the same or different types.

Alternatively the GUP Component may contain zero or more Data Elements without the Data Element Groups. A GUP component shall have at least one Data Element Group or Data Element.

A Composite Datatype is used to define the structure of the whole GUP Component. The structure includes definition about what kind of Data Element Groups and/or which Data Elements belong to the defined GUP Component as well as the data types and valid values of the data.

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

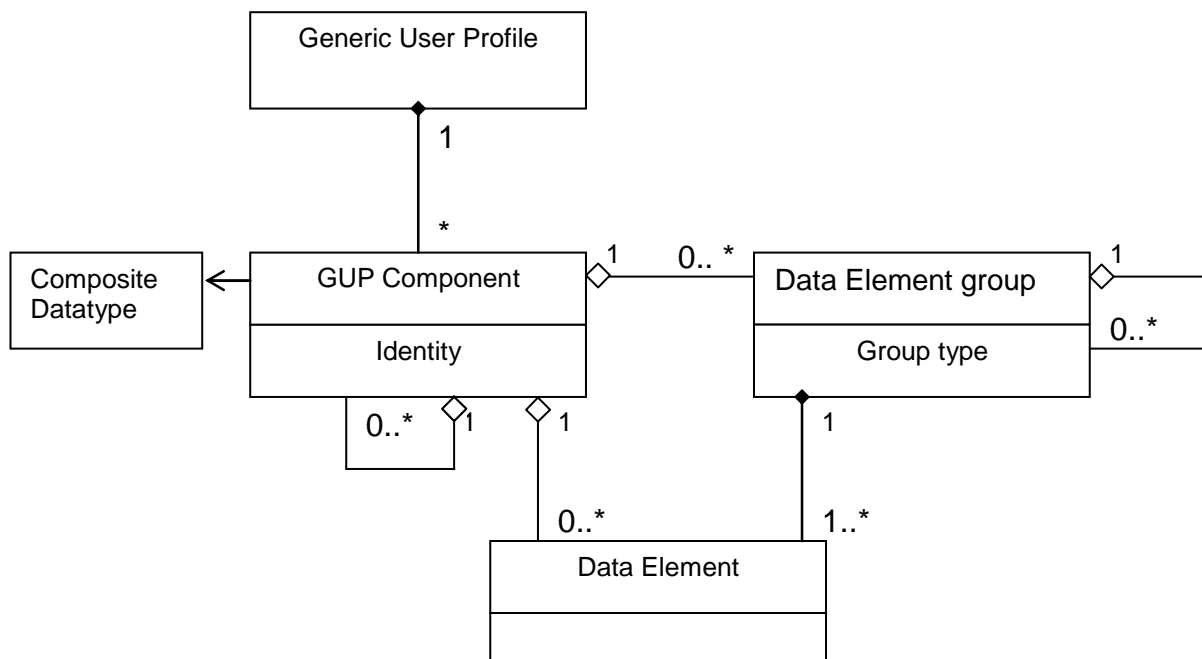


Figure 5.1: The basic concepts of GUP

GUP defines an Authorisation Component, which is just like any other GUP Component. This implies that the same capabilities as for any GUP Component (e.g. identities and structure) are also applied to the Authorisation Component. The Authorisation Component is able to reference any element of the GUP Information Model and define the authorisation regarding those elements. The Authorisation Component may be either subscriber specific or common to several subscribers and/or elements of the GUP Information Model.

Note that any GUP Component may include additional data items, which are used (e.g. by RAF) for the authorisation purposes but those are seen as a part of the data specific to a certain GUP Component, and thus not a part of the generic authorisation specified by GUP.

Figure 5.2 presents an example structure of Generic User Profile with the terms used in the UML Class Diagram. Note that the data structure may be also deeper than shown in the example figure, e.g., the Data Element Groups might consist of nested Data Element Groups.

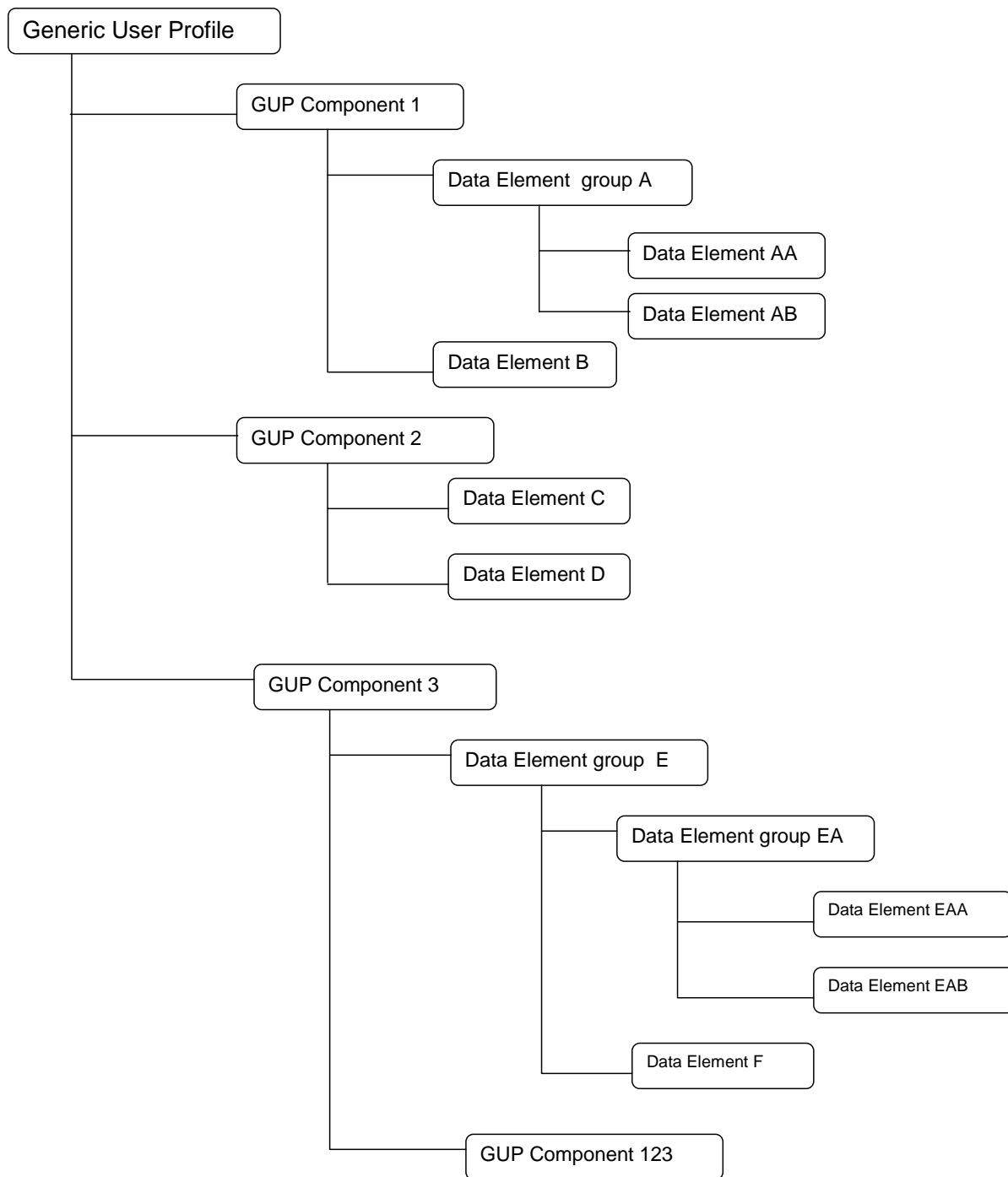


Figure 5.2: Example structure of GUP information

One purpose of the example structure is to clarify the intended relation between the UML Class Diagram and the hierarchical structure of GUP in terms of XML. Use of XML fulfils the requirements for the architectural structure of the GUP information model.

Each Generic User Profile consists of one or several GUP Components depending on the nature of the user related data. GUP Components are independent XML documents. The Generic User Profile is thus formed of a number of XML documents.

Each GUP Component consists of GUP Components, Data Elements and/or Data Element Groups as defined in the component specific definitions. In XML terms the Data Elements are XML elements. The Data Element Group is a structured XML element with an arbitrarily deep data structure.

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

Example 1: GUP Usage with Subscription Management

An application is accessing targeted subscriber's subscription data (HSS GUP Component) stored in the HSS. It is assumed that RAF is implemented in the HSS and the targeted HSS GUP Component has been created by using the Create Component procedure. The application in this case can be e.g. a Subscription Management application, a service application or any third party application that is interested in the subscription data of a specific subscriber in operator A's network.

The example of the interworking interface diagram is shown in Figure A.2. In this example GUP Server is working in the proxy mode of operation.

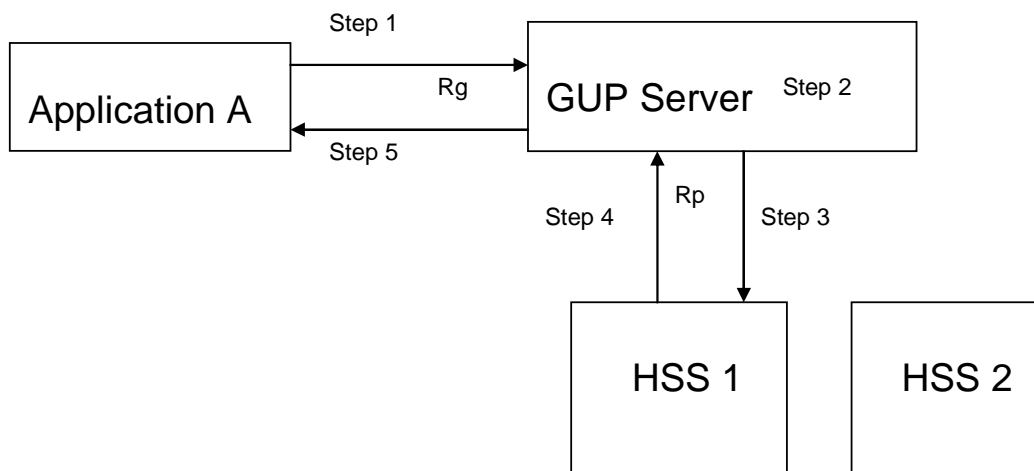


Figure A.2: An Example of the Interworking Diagram between GUP and an Application

The interworking steps between the Application, GUP Server and HSS are summarised below:

Step 1: Application A invokes a Query procedure to the GUP Server including the targeted subscriber's public user identity `joe.doe@operatorA.com` in the Resource Identity parameter. The HSS GUP Component will be included in the Data Reference parameter clarifying the targeted data (component type) that the application is interested in. Also specific data (i.e. XML Data Element) within one GUP Component can be requested. Application A's identity is included in the Requestor data parameter for the identification and authorisation purposes of the request.

Step 2: GUP Server authenticates the application and authorises the request with the result that Application A is allowed to access the HSS GUP Component of the subscriber `joe.doe@operatorA.com`.

Step 3: GUP Server locates the target GUP Data Repository (RAF address), i.e. that the HSS GUP Component of the subscriber `joe.doe@operatorA.com` is located in the HSS 1, and invokes Read data procedure to HSS 1.

Step 4: HSS 1 makes an internal query by using the public user identity `joe.doe@operatorA.com` and returns a response to Read data procedure to the GUP Server including the requested HSS GUP Component data of the subscriber `joe.doe@operatorA.com`.

Step 5: GUP Server passes the received response to Query procedure further to Application A.

The GUP Server may retrieve authorisation GUP Components from a RAF, if it does not hold sufficient information by itself to carry out the authorisation.

If necessary, e.g. when the application requests several GUP Components, or the whole profile including several GUP components in different repositories, GUP Server can invoke several requests to various RAFs and combine responses to one response when returning a response to the application.

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

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 categorization of the data in the table does not imply similar GUP component structure.

GUP access	Supplier	Data repository	Description of the data	Consumer
General user data for IMS	AS manager	AS	ISIM subscriber data for IMS: <ul style="list-style-type: none"> - 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 	S-CSCF
MMS VASP applications Ref TS 23.141 [7]	AS manager	AS	MMS application specific data: <ul style="list-style-type: none"> - Authorization - Confidentiality - Charging information - Message distribution 	MMS server
Privacy control settings of the user	AS manager	AS	Privacy control data of the user: <ul style="list-style-type: none"> - Privacy settings for standardized service like Presence - Privacy setting of non standardized services 	UE-ISIM
PLMN specific user information	O&M	HSS	PLMN specific user information: <ul style="list-style-type: none"> - 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
Authorized and subscribed service information for CS & PS	O&M HSS-HLR	HSS-HLR	Authorized and subscribed service information: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Forwarding & barring information - CAMEL subscription information 	CSE
Authorized and subscribed service information for IMS	O&M	HSS	Authorized and subscribed service information: <ul style="list-style-type: none"> - IM Subscriber ID (Private User ID, Public ID) - Subscribed media - Billing policy - Initial filter criteria - Service keys & triggering aspects - Authorized services that the subscriber may subscribe to - Services the subscriber actually has subscribed to 	S-CSCF AS
CAMEL services for IMS	O&M	HSS-HLR	CAMEL subscription information for IMS	IM-SSF

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2003-06	SA#20	SP-030310			Raised to v.6.0.0 after approval at SA#20	2.0.0	6.0.0
2003-09	SA#21	SP-030381	001	1	Rg reference point compliance with Liberty Alliance Project ID-WSF	6.0.0	6.1.0
2003-09	SA#21	SP-030381	002	1	Introduction of discovery service	6.0.0	6.1.0
2003-09	SA#21	SP-030381	003	1	Corrections to Rg reference point descriptions	6.0.0	6.1.0
2003-09	SA#21	SP-030381	004	1	Removal of GMLC as example	6.0.0	6.1.0
2003-12	SA#22	SP-030659	007	1	Selection of the GUP Server mode of operation	6.1.0	6.2.0
2003-12	SA#22	SP-030659	009	1	Notification Reference	6.1.0	6.2.0
2003-12	SA#22	SP-030659	010	2	Subscribe Operation, Subscription Status	6.1.0	6.2.0
2003-12	SA#22	SP-030659	011	1	GUP information model improvement	6.1.0	6.2.0
2003-12	SA#22	SP-030659	012	1	GUP Annex B terminal Capability negotiation for IMS	6.1.0	6.2.0
2004-03	SA#23	SP-040038	006	4	Adding a listing function	6.2.0	6.3.0
2004-03	SA#23	SP-040038	013	2	Rg reference point alignment with Liberty ID-WSF	6.2.0	6.3.0
2004-03	SA#23	SP-040038	014		Generalizing the subscriber identity term to resource identity	6.2.0	6.3.0
2004-03	SA#23	SP-040038	015	1	Authorization enhancements	6.2.0	6.3.0
2004-03	SA#23	SP-040038	016		Authorization model alignment with GUP Information Model	6.2.0	6.3.0
2004-06	SA#24	SP-040321	017	1	GUP Server in Home operator network	6.3.0	6.4.0
2004-06	SA#24	SP-040321	018	1	Rp Intra-operator interface	6.3.0	6.4.0
2004-06	SA#24	SP-040321	019	1	GUP Authentication failure	6.3.0	6.4.0
2004-06	SA#24	SP-040321	020		Removal of editor's note on existing profile components	6.3.0	6.4.0
2004-06	SA#24	SP-040321	021	1	Addition of an example in Annex A	6.3.0	6.4.0
2004-06	SA#24	SP-040321	022	2	Clarification of requirement for component location management	6.3.0	6.4.0
2004-09	SA#25	SP-040525	024	1	Addition of missing security aspects	6.4.0	6.5.0
2004-12	SA#26	SP-040757	025		Removal of UE as GUP Data Repository	6.5.0	6.6.0
2005-03	SA#27	SP-050109	026		Use of Discovery Service as Trusted Authority	6.6.0	6.7.0
2007-06	SP-36	-	-	-	Update to Rel-7 version (MCC)	6.7.0	7.0.0
2008-12	SP-42	-	-	-	Update to Rel-8 version (MCC)	7.0.0	8.0.0
2008-12	SP-46	-	-	-	Update to Rel-9 version (MCC)	8.0.0	9.0.0
2011-03	SP-51	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	11.0.0
2014-09	SP-65	-	-	-	Update to Rel-12 version (MCC)	11.0.0	12.0.0
2015-12	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	13.0.0
2017-03	-	-	-	-	Update to Rel-14 version (MCC)	13.0.0	14.0.0
2018-06	SP-80	-	-	-	Update to Rel-15 version (MCC)	14.0.0	15.0.0
2020-07	SP-88E	-	-	-	Update to Rel-16 version (MCC)	15.0.0	16.0.0
2022-03	SP-95E	-	-	-	Update to Rel-17 version (MCC)	16.0.0	17.0.0

History

Document history		
V17.0.0	April 2022	Publication