3GPP TSG SA WG3 (Security) meeting #30 **S3-030581**

6-10 October 2003

Povoa de Varzim, Portugal

Source:	**Nokia**
Title:	**GUP security directions**
Document for:	**Discussion**
Agenda Item:	**7.17**

Introduction

The present contribution is provided to start the work on the Generic User Profile (GUP) Security. The Rel-6 GUP stage 2 specification TS 23.240 was approved by SA#20. CN4 has also started work on the stage 3 TS 29.240 and T2 continues their efforts on the Data Description Method (DDM). We see that it is now possible to start the GUP security work in SA3. This contribution provides a short introduction to GUP architecture and our general ideas on the related security work.

Discussion

The GUP architecture is depicted in TS 23.240 as shown below in figure 1.

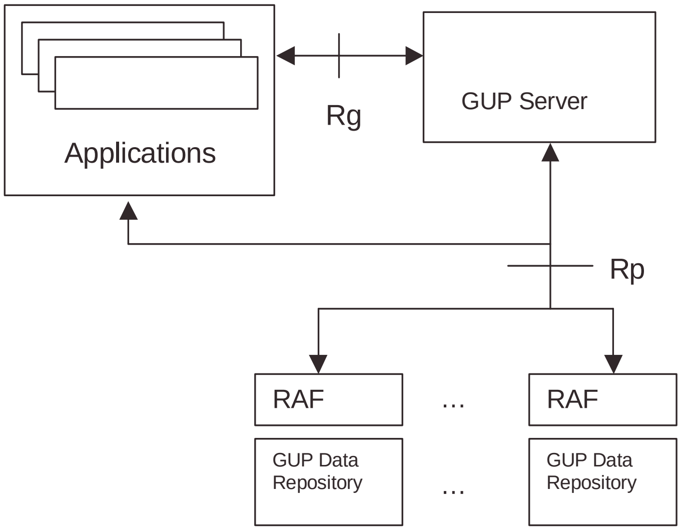


Figure 1. The GUP architecture

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

Reference Points in the GUP Reference Architecture:
1. Reference point Rg
This reference point shall allow applications to create, read, modify and delete any user profile data using the harmonized access interface. The GUP Server locates the data repositories responsible of the storage of the requested profile component(s) and in case of proxy mode carries out the requested operation on the data.
In the redirect mode, the GUP Server returns the locations of the GUP Data Repositories and the application can then send the requested operations via reference point Rp directly to the corresponding GUP Data Repositories.
The reference point Rg carries user related data, and therefore shall be protected by security mechanisms.

2. Reference point Rp
This reference point shall allow the GUP Server or applications, excluding third party applications, to create, read, modify and delete user profile data using the harmonized access interface. Third party applications and third party GUP data repositories shall be connected to the GUP Server only using the Rg reference point.

The reference point Rp carries user related data, and therefore shall be protected by security mechanisms.

CN4 has made a working assumption to apply SOAP protocol in both Rp and Rg.

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

The main tasks in the security area are:

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

Clearly the first two belong to SA3's scope but also authorisation is included in the SA3 GUP Security WID and it involves aspects (e.g. assertion usage) where the expertise of SA3 would be highly valuable. Related to authorisation TS 23.240 defines a requestor data parameter in several operations to provide information about the requestor e.g. end user and application identification, credentials, authorisation assertions or privacy policy information.

There has been a common view that Liberty Alliance Project work (especially phase 2) should be taken into account and utilised where possible. The Liberty Identity Web Services Framework (ID-WSF) and ID Personal Profile have very similar tasks as GUP and SOAP is also applied in both. Hence we feel that especially the third party access security can be based on the Liberty Alliance Project specifications. Discovery service plays a central role in authorisation in Liberty ID-WSF. Our earlier contribution **S2-031986** gives some more views on the GUP and Liberty ID-WSF relationship. Note however that this has not been approved by SA2 as such. The Discovery service of Liberty Alliance Project is mentioned as an example but not mandated as such by TS 23.240.

A few relevant Liberty Alliance Project specifications:

- Liberty Security & Privacy Overview
- Liberty ID-WSF Security Mechanisms
- Liberty Authentication Context Specification
- Liberty SASL-based SOAP Authentication Specification

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

See http://www.projectliberty.org/ for more information on Liberty Alliance Project. Note that the phase 2 specifications will be frozen only later this year.

Proposal

We propose that SA3 would discuss how the GUP security work will be handled supporting the work of CN4 (and SA2) and decide what would be the scope, contents and format (e.g. CRs to TS 23.240

and TS 29.240). We see that CN4 specifications should be mentioned in the SA3 GUP Security WID as well.

Futhermore we suggest that SA3 would consider taking the Liberty Alliance Project ID-WSF security solutions as the basis for the work.

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

7 Security

Secure mechanisms shall be available for the transfer of User Profile data to, from or between authorised entities. Access to User Profile data shall only be permitted in an authorised and secure manner. The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.
The secure mechanisms available shall include the following:

1. Authentication of recipient
   Before any user data transfer takes place, it shall be possible for the sender of the data to verify the identity of the recipient.

2. Authentication of sender
   It shall be possible for the recipient of data to identify the sender.

3. It is permissible for either the sender or recipient of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.

4. The validity of an authentication of identity shall, if required, be subject to a maximum time limit.

5. It shall be possible for the sender of data to render the data to be unreadable by any party not authorised to receive it.

6. It shall be possible for the recipient of data to detect whether the sender has made any change to the data subsequent to its transmission.

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

8. It shall be possible for the sender and/or the recipient to create an audit log of all data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place

9. User profile data in general is proprietary data. This data may not be shared with unauthorized entities. *Access control* to the data is required. This access control must also apply to data which is located at legacy systems, currently without own access control functionality.

10. Correct setting of data values in the user profile may be critical for the integrity of certain network services. Therefore, *consistency checks* are needed to minimise the risk.

11. Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.

8 Privacy and Authorisation

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

8.1 General Requirements

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

The privacy requirements shall fulfill local privacy regulations. Lawful interception and other regulator requirements may imply that GUP data is delivered to authorities despite the privacy settings.

8.2 Authorisation Rules

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

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

The disclosure of the user profile data must be considered based on the identification of the application requesting access to the data. The possible identities of the applications will not be standardised but are implementation specific.

Regarding trusted applications involving other subscribers or comparable entities it shall be possible also to check the access rights of the subscriber being served by the application. This requires that the identification of the served subscriber is passed via the GUP mechanism in addition to the application identification. The access is first defined per applications and secondly per served subscriber. The access may be granted also to the public, some group or a list of subscribers.

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

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

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

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

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

4.1.3 Authentication of profile access

A GUP functionality exists that is responsible to authenticate applications. Authentication is a vital function to be passed before any kind of access to GUP data is granted. GUP shall adopt generic mechanisms such as used for the OSA framework approach.

4.1.4 Authorization of profile access

A GUP functionality exists that is responsible to authorise applications to access GUP data based on User specific privacy rules. All attempts to access the GUP data are to be authorized according to the defined policies which shall include the requestor's identity.

The GUP data structures need to satisfy the requirement to provide the authorization information on the different levels: profile, component or data element. In addition to the generic authorization data, additional service specific data may be defined (e.g. for LCS). The same applies for the authorization decision logic. How the generic decision logic is defined and provided is FFS.

Both HPLMN based applications and non-HPLMN based applications are expected to send requests to the GUP Server. The GUP server shall have functionality to apply different authorization criteria, policy control and load control to HPLMN and non-HPLMN applications. Policy control and load control are out of the scope of the present document.

4.1.5 Privacy control

The tight connection of authentication, authorization and subscriber specific privacy requirements results in privacy control. Privacy control implies a centralized management for access rights including the subscriber's privacy requirements.

4.2.1.3 Authentication of profile request

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

4.2.1.4 Authorization of profile request

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

3GPP TSG-SA WG2 Meeting #32 S2-031980
San Diego, USA, 12 – 16 May 2003 Agenda Item: 9.1

Title: Liberty Alliance Project specifications relationship to GUP

Source: Nokia

Document for: Discussion and approval

1. Introduction

This contribution discusses the recently released Phase 2 drafts of the Liberty Alliance Project and their relationship to GUP. It is proposed that Rg reference point of GUP would be made Liberty Identity Web Services Framework compliant.

2. Discussion

2.1 Liberty Alliance Project introduction

Liberty Alliance Project http://www.projectliberty.org/ is a standardisation organisation of about 150 members. The specifications provide broad range of identity based services such as single sign-on and personal profile. The user interacting with WWW services and web services in general are the main target areas.

The Liberty Alliance specifications can be divided into three parts: Liberty Identity Federation Framework (ID-FF), Liberty Identity Web Services Framework (ID-WSF) and Liberty Identity Services Interface Specifications (ID-SIS).

ID-FF supports several configurations to provide e.g. single sign-on and logout features for the user accessing different web services (or potentially any other services). When a user is accessing a Liberty enabled web service it may request user credentials from the IDP. The user must be authenticated to the Identity Provider (IDP) by some means (not specified by Liberty) before the IDP can provide any credentials to the web service. Anonymity is fully supported by the IDP that can generate different user identifications for different services. SAML specified by OASIS is extensively applied in ID-FF /SAML/.

ID-WSF is a completely new part in Liberty specifications that was just recently published as part of the Liberty Phase 2. It provides a framework for creation of identity services related to the attributes attached to the identity. User profile can be regarded as one identity service.

The ID-SIS part specifications contain currently one concrete Identity Personal Profile Service /IDPP/ that has been specified based on the ID-WSF. Other user profile (e.g. GUP) or other attribute services can be specified according to ID-WSF.

2.2 Liberty Identity Web Services Framework

The Liberty Identity Web Services Framework (ID-WSF) outlines the technical components necessary to build interoperable identity-based web services. Specific features include (see /LIBAW/):

- *Permissions-Based Attribute Sharing* - This allows an organization to offer users individualized services based on attributes and preferences that the user has chosen to share.

- *Identity Discovery Service* – This allows a service provider to dynamically discover the location of a user's identity services, and for the identity provider to respond based on the user's permissions. This feature is critical for being able to offer a large number of users real-time identity-based services.

- *Interaction Service* – This allows an identity service to obtain permission from a user (or someone who owns a resource on behalf of that user) to allow them to share data with the requesting service.

- *Security Profiles* – This describes the profiles and requirements necessary to protect privacy and ensure the integrity and confidentiality of messages.

- *Extended Client Support* – This enables hosting of Liberty-enabled identity-based services on devices without requiring HTTP servers. This is useful since most consumers do not run HTTP-servers on their PCs, and many networks do not support running HTTP servers on consumer devices. This also reduces implementation costs in resource-constrained devices such as mobile phones.

The figure1 shows the Liberty ID-WSF architecture. The figure contains also the IDP but this contribution concentrates on the ID-WSF part. First there is a Discovery Service (DS) that holds information about the different Identity Services i.e. Web Service Providers (WSP) that provide information about users. Discovery Service specifies *Discovery Update* to register the information from the WSP to the DS. *Discovery Lookup* is applied by the Web Service Consumers (WSC) to get the reference and assertions to the WSP. The identity which is applied by the WSC may be different from the one that is provided by the DS to be sent to the WSP when accessing the identity information. For more information on the Liberty Discovery Service see /DISCO/.

The ID-WSF Data Service Template /DST/ defines the identity protocol between WSC and WSP. In functional sense two operations (with corresponding responses) are defined: Query and Modify. What is actually defined are the XML data elements that are to be transmitted in the SOAP message body /SOAPB/.

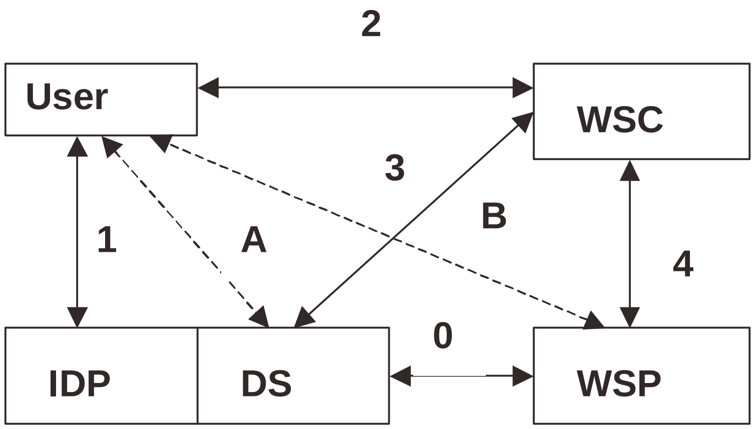


Figure 1. ID-WSF architecture including the Identity Provider (IDP), Discovery Service (DS), Web Service Consumer (WSC) and Web Service Provider (WSP).

Let's go through the functions in figure 1 step by step:

- First a relationship between the IDP, DS and WSP is established. It is foreseen that often IDP and DS are co-located and initially the subscriber has somekind of relationship to the IDP e.g. by means of mobile network or some off-line agreements and shared secret credentials for authentication.

- WSP registers its user data Service Instances with the DS (0)

- When a user starts using a service offered by WSC, she must first be authenticated. This may happen by the means of Liberty ID-FF or by other means. The user may have been first authenticated to IDP (1) and then to WSC via authentication request redirection to IDP (2). There are also other alternatives.

- WSC discovers (3) the Service Instance that is able to provide the subscriber profile data (attributes) needed for the service. DS checks the WSC's authorisation to the access before giving the WSP information. It is presumed that DS has authenticated WSC (and optionally also vice versa).

- WSC fetches (4) the profile data from the WSP which checks the authorisation. It is presumed that WSP has authenticated WSC (and optionally also vice versa).

- WSC is able to provide the best service for the user based on the profile data

The dashed lines in the figure 1 show the user interacting with the DS and WSP e.g. to provide some attributes or authorisation information. Also the interaction service specified by Liberty may be optionally applied in these interfaces (A and B) to get user’s consent for some actions.

2.3 Motivations to apply Liberty specifications in GUP

It has been acknowledged both in Liberty Alliance Project and 3GPP SA1 and SA2 that there is a need for establishing a liaison relationship between these organisations to prevent overlapping specification work and to make referencing to each other’s specifications possible. LCS has been one area where anonymity and credential/assertion features of Liberty have been deemed relevant for 3GPP.

The following things speak for using Liberty specifications in GUP:

- Ready made for similar purpose, especially Rg
- Covers many of the GUP requirements and maps well with the GUP architecture
- Overlapping specifications avoided
- Discovery and third party support provided by Liberty specifications
- Good authorisation and privacy solutions
- Mainstream technology choices well applicable to GUP
- Extensible and easy to adapt to cover GUP requirements
- Based on proven Liberty concepts

2.4 Liberty mapping to GUP architecture

The Liberty ID-WSF provides a set of web services specifications. In our view this technology seems to match very well with the need of the Rg reference point of GUP. On the other hand Rp reference point has some needs and characteristics (e.g. efficient subscriber data management by operator) that are not fully supported by Liberty ID-WSF. Rp has been defined for operator’s own use only and the core network elements have to be secured well enough from the outside. However it is beneficial to keep Rg and Rp procedures as close to each other as possible. The profile component data should naturally be identical in these interfaces.

The figure 2 shows how Liberty ID-WSF can be mapped to GUP architecture. The Discovery Service (DS) has been added with two new reference points Rr and Rd. We propose that the Liberty discovery specification /DISCO/ would be endorsed i.e. referenced as is by 3GPP without any additional requirements or descriptions.

Rr is the registration reference point which is used by the GUP server to register its Rg protocol endpoint to the Discovery Service. Rr covers e.g. *Discovery Update* in /DISCO/.

Rd is the discovery reference point which is used by the applications to discover the Rg endpoint (GUP Server). Rd covers e.g. *Discovery Lookup* in /DISCO/.

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. Third party applications may need to use discovery as a normal step, but in operator’s services it may not be always needed. Discovery also provides part of the authorisation.

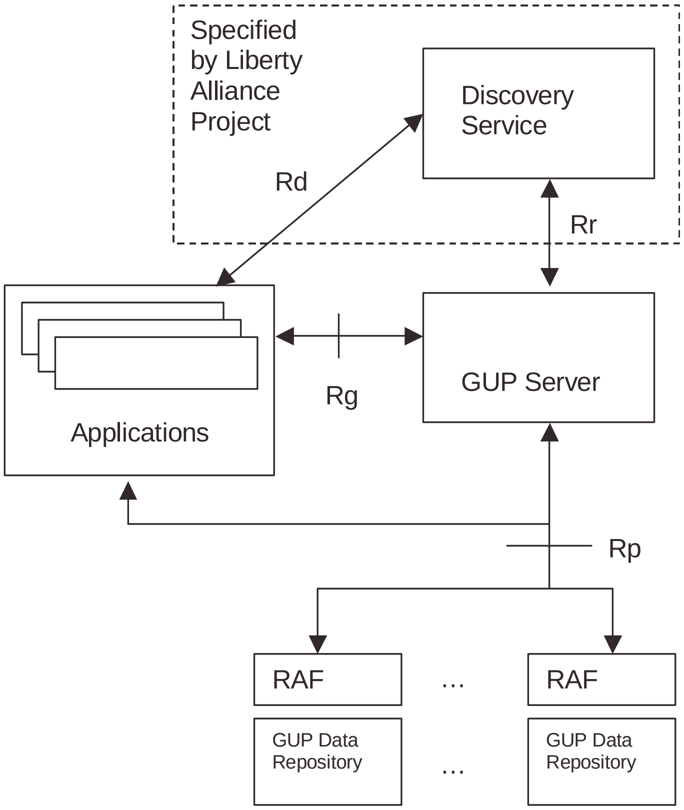


Figure 2. Liberty ID-WSF mapping to GUP architecture

It should be noted that several GUP servers may register themselves to the DS.

In our view Liberty ID-WSF Data Service Template /DST/ framework should be applied without changes in Rg reference point. Additional functions are however needed for e.g. create, delete and synchronisation. Create function can be used to create a new user profile or add components to an existing one. They can be defined in the same way as /DST/ now defines query and modify protocols. Furthermore the GUP Profile Service shall be made up. /IDPP/ can be taken as a reference but also other technical solutions in the details are possible within the framework of ID-WSF. The user profile shall consist of separately defined component schemas (e.g. for IMS subscription data in HSS) with a possibility to add new standardised or proprietary components.

The key parameters in the /DST/ protocols are the following:

- Resource. Indicates e.g. the user.
- Select. Identifies which data are concerned. ID-WSF /DST/ does not specify the exact type of contents because it is service specific.
- NewData/Data. Contains the modified/queried data.

These parameters can be well applied to fulfill also GUP requirements.

2.5 Security and privacy

Security and privacy assurance are key features in the Liberty work. See /SECP/ and /SECG/. A short overview is given here. Liberty refers mostly to the existing technologies (e.g. SSL, TLS, SAML and X.509) giving instructions how those are to be applied in this framework.

SSL 3.0 or TLS are suggested as the the transport security framework on top of which Liberty specific security measures are employed. XML encryption can be used for message encryption and integrity protection and non-repudiation can be provided by XML signatures. Either Public Key Infrastructure (X.509) based keys or shared secret keys as well as SAML Assertion Layer Sender Authentication can be applied.

All the parties (principal of the data, IDP, DS, WSP and WSC) involved in the identity attribute handling must be properly authenticated before any access is granted. Servers are usually authenticated based on server certificates. Liberty does not explicitly define how the user/principal is authenticated with the IDP. If active intermediaries are present, messaging layer authentication may have to be used.

Privacy is ensured by properly authorising the entities that access the user data. Use of pseudonyms is an inherent part of Liberty identity services. The basic principle is that each service (e.g. WSC) gets different user identifications for the same user and these can be also encrypted (i.e. only readable by IDP/DS and WSP) and different each time when retrieved to make tracking impossible. It is said that the different entities have different namespaces which are correlated by the IDP/DS.

In Liberty architecture the authorisation of WSC happens in two stages:

- Discovery Service authorises the WSC access to the WSP
- WSP authorises the WSC access to the user (attribute) data.

The Discovery Service may also provide SAML assertions/tokens for the WSC to be given to the WSP.

The *usage directive* in SOAP header may carry privacy policy data to e.g. tell if the data may be transmitted to third parties or not.

2.6 References

All the below mentioned draft specifications can be found at: http://www.projectliberty.org/

/LIBAW/ Introduction to the Liberty Alliance Identity Architecture

/DST/ ID-WSF Data Service Template

/DISCO/ Liberty Discovery Service Specification

/IDPP/ Liberty Identity Personal Profile Service Specification

/SOAPB/ Liberty ID-WSF: SOAP Binding

/SECP/ Liberty ID-WSF Security Profiles

/SECG/ Liberty Security & Privacy Implementation Guidelines

Additional OASIS reference:

/SAML/ OASIS, Security Assertion Markup Language (SAML), http://www.oasis-open.org/

3. Proposal

We kindly propose to make a reference to Liberty Alliance Project specifications regarding the GUP Rg reference point. We realise that the official liaisonship between 3GPP and Liberty Alliance Project has to be finalised before a reference to Liberty specifications can be included in the approved GUP specification. The suggested changes to TS 23.240 are given below.

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)".

[2] Liberty Discovery Service Specification, http://www.projectliberty.org/

[3] Liberty ID-WSF Data Service Template, http://www.projectliberty.org/

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.

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:

Rd	Reference Point between Applications and the Discovery Service
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.
Rr	Reference Point between the GUP Server and the Discovery Service

3.3 Abbreviations

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

GUP	3GPP Generic User Profile
RAF	Repository Access Function
DS	Discovery Service

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. A discovery service defined by Liberty Alliance Project [2] may be used to get the contact reference information of 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.

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

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 synchronisation. 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.

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

Synchronisation 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 synchronisation as fast as possible. All the unresolved errors or load balancing actions that affect synchronisation 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.

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.

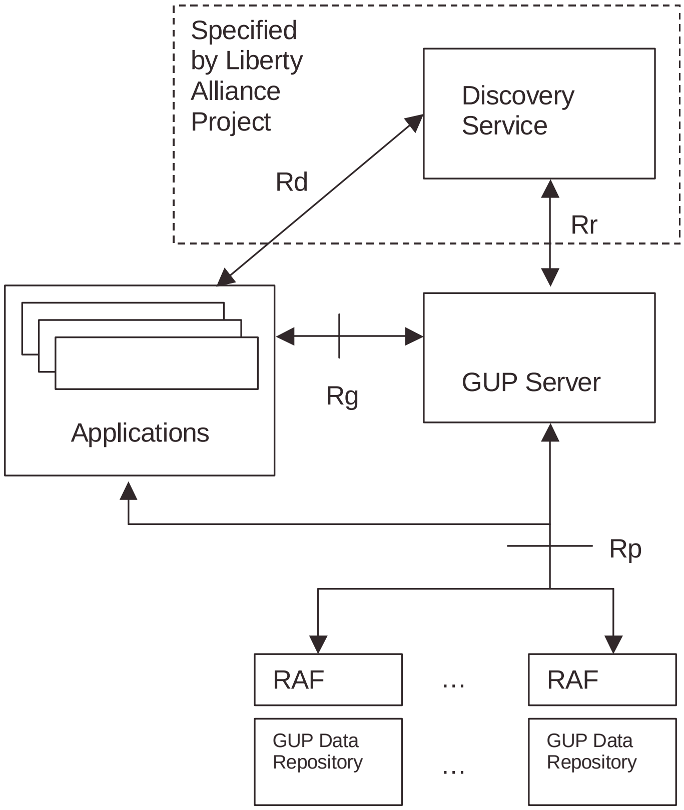
NOTE: GUP Data Repositories within a UE are not expected to produce charging information.

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;
- Rd, Rg, ~~and~~ Rp and Rr reference points;
- ~~–~~Applications.
- Discovery Service (DS)



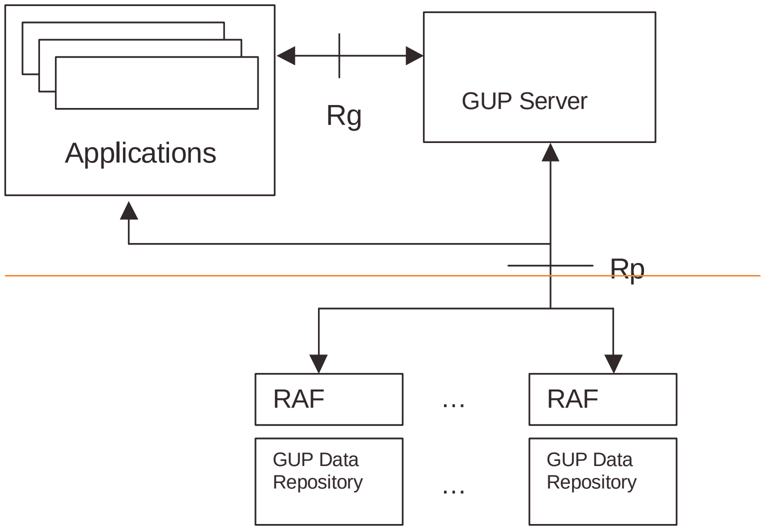


Figure 4.1: GUP Reference architecture

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

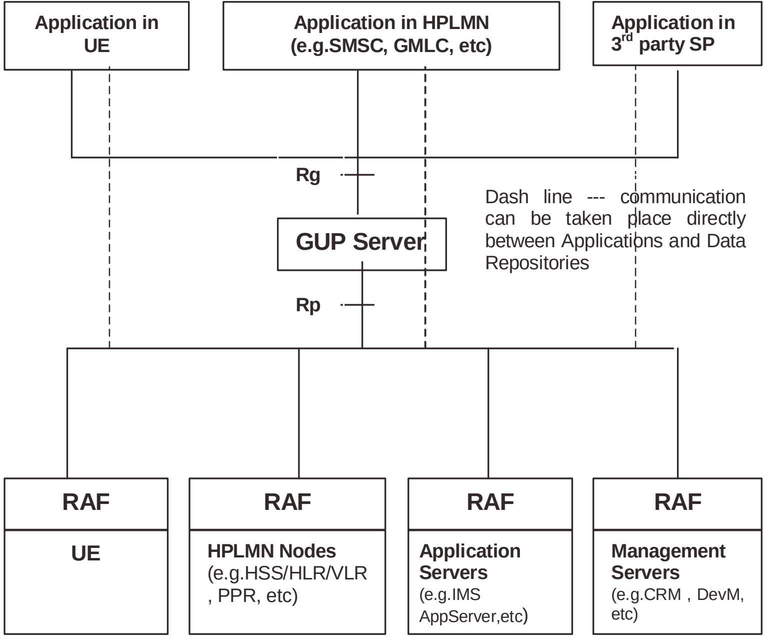

Application in UE
Application in HPLMN (e.g.SMSC, GMLC, etc)
Application in 3rd party SP
Rg
GUP Server
Dash line --- communication can be taken place directly between Applications and Data Repositories
Rp
RAF
UE
RAF
HPLMN Nodes (e.g.HSS/HLR/VLR, PPR, etc)
RAF
Application Servers (e.g.IMS AppServer,etc)
RAF
Management Servers (e.g.CRM , DevM, etc)

Figure 4.2: An example of mapping the GUP reference architecture to Current Infrastructure Environment (note that DS has been omitted for simplicity)

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 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.
- Authorisation of profile requests.
- Synchronisation of Profile Components.

Editor's note: Texts about the operation mode of the GUP Server shall be added here. Whether the GUP Server is implemented as a Proxy and/or Redirect Server must be defined later, see the two figures below.

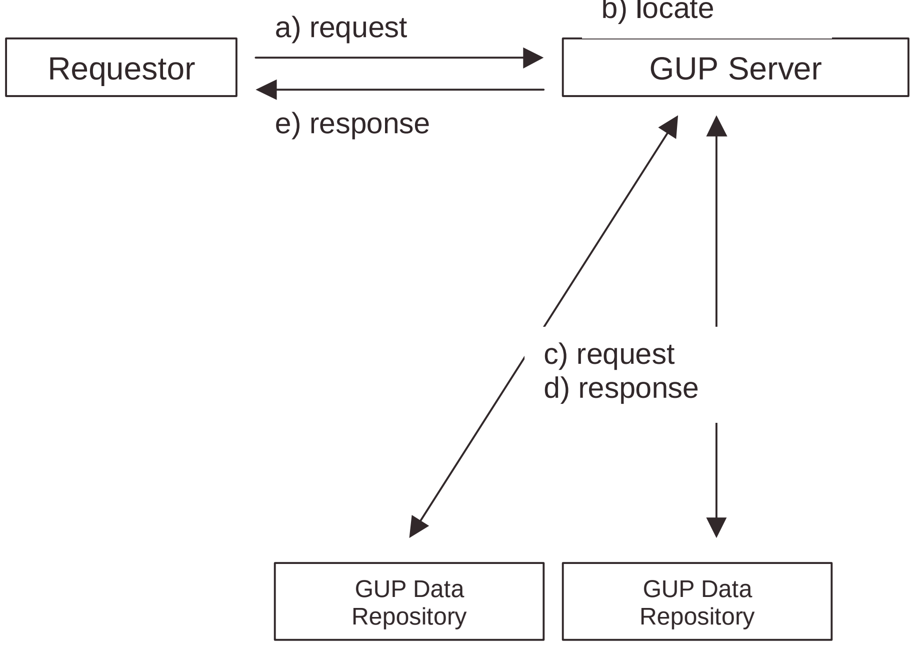


Figure 1. GUP Server acting as a Proxy Server.

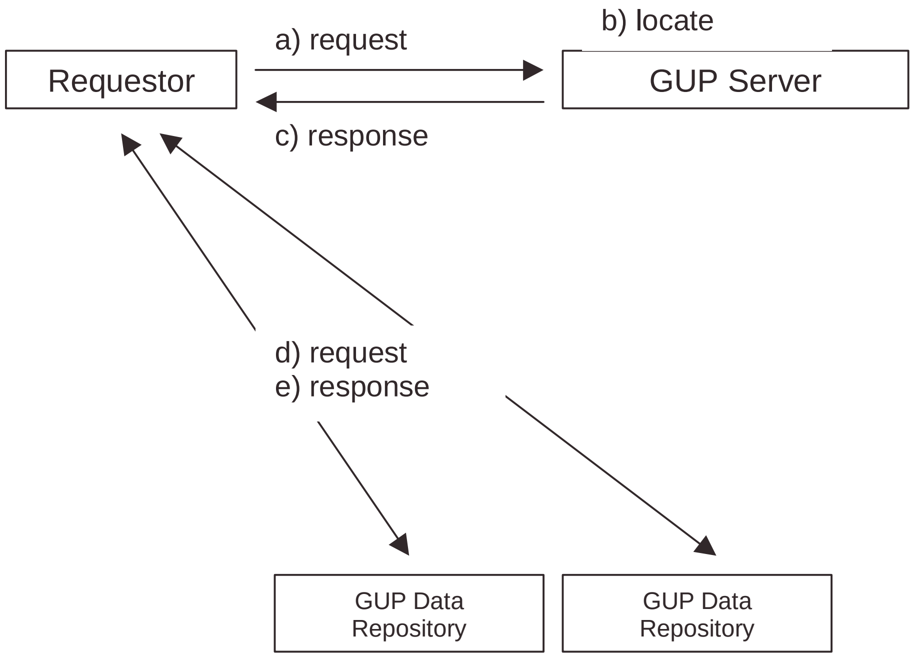


Figure 2. GUP Server acting as a Redirect Server.

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

Editor’s note: the Proxy Server mode of operation is assumed in the texts below. When the decision of the Proxy vs. Redirect mode of operation is selected the texts might need to be updated accordingly.

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 convey the corresponding GUP Component specific requests to GUP Data Repositories via Rp reference point. Note that one data request from an application can cause sending of several GUP Data Repository requests by the GUP Server. Also mapping to proprietary interfaces instead of Rp is possible in implementations.

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.

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. 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 Authorisation of Profile Request

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

4.2.1.5 Synchronisation of Profile Components

The GUP Server shall convey the data synchronisation 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 synchronisation requests implemented.

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.

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 GUP Data Repository

Each GUP Data Repository stores the primary master copy of one or several profile components. The RAF provides for the standardised 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.

4.2.4 Discovery Service

The Discovery Service (DS) is able to receive register requests from service instances (i.e. GUP Servers) that offer user profile access over Rg reference point. DS also provides an interface for the applications to discover the registered services that are able to provide access to the profile data of the specified users. Discovery Service is specified by the Liberty Alliance Project [2].

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. Third party applications may need to use discovery as a normal step, but in operator's services it may not be always needed. Discovery also provides part of the authorisation.

4.2.~~4~~5 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. Rg is specified in compliance with the Liberty Identity Web Services Framework (ID-WSF) [3].

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.

3. Reference Point Rr

This reference point shall allow GUP servers to register their protocol endpoints for different users' profile data access. Liberty Discovery Service Specification [2] is applied as such.

4. Reference Point Rd

This reference point shall allow applications to discover the protocol endpoints for different users' profile data access. Liberty Discovery Service Specification [2] is applied as such.

4.2.~~5~~6 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. Applications have different authorisation rights to the GUP data of different subscribers as agreed between the parties.

4.2.~~6~~7 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 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 4.3 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. However the GUP Server must never “bypass” existing privacy rules.

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

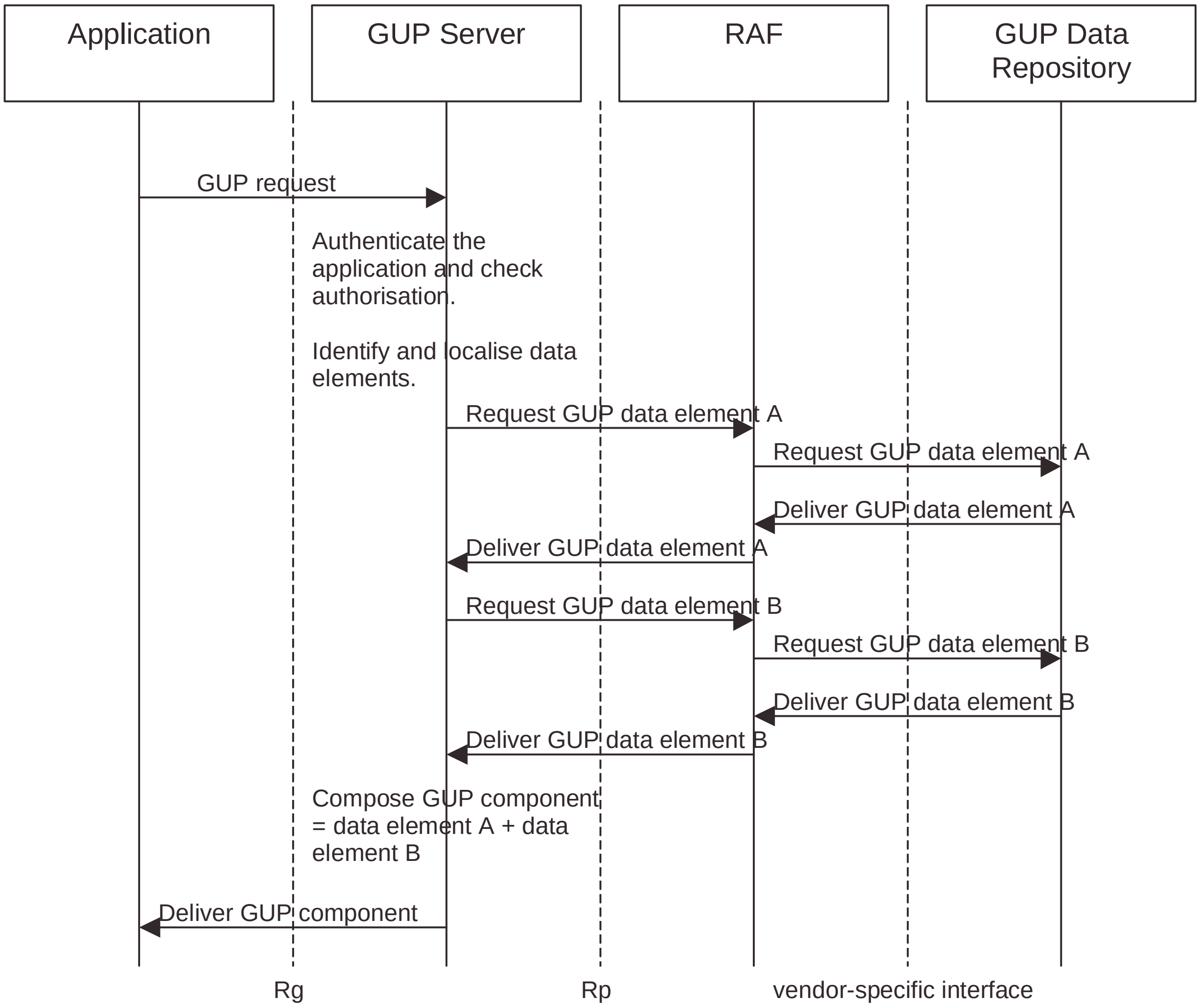

Application
GUP Server
RAF
GUP Data Repository
GUP request
Authenticate the application and check authorisation.
Identify and localise data elements.
Request GUP data element A
Request GUP data element A
Deliver GUP data element A
Deliver GUP data element A
Request GUP data element B
Request GUP data element B
Deliver GUP data element B
Deliver GUP data element B
Compose GUP component = data element A + data element B
Deliver GUP component
Rg
Rp
vendor-specific interface

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

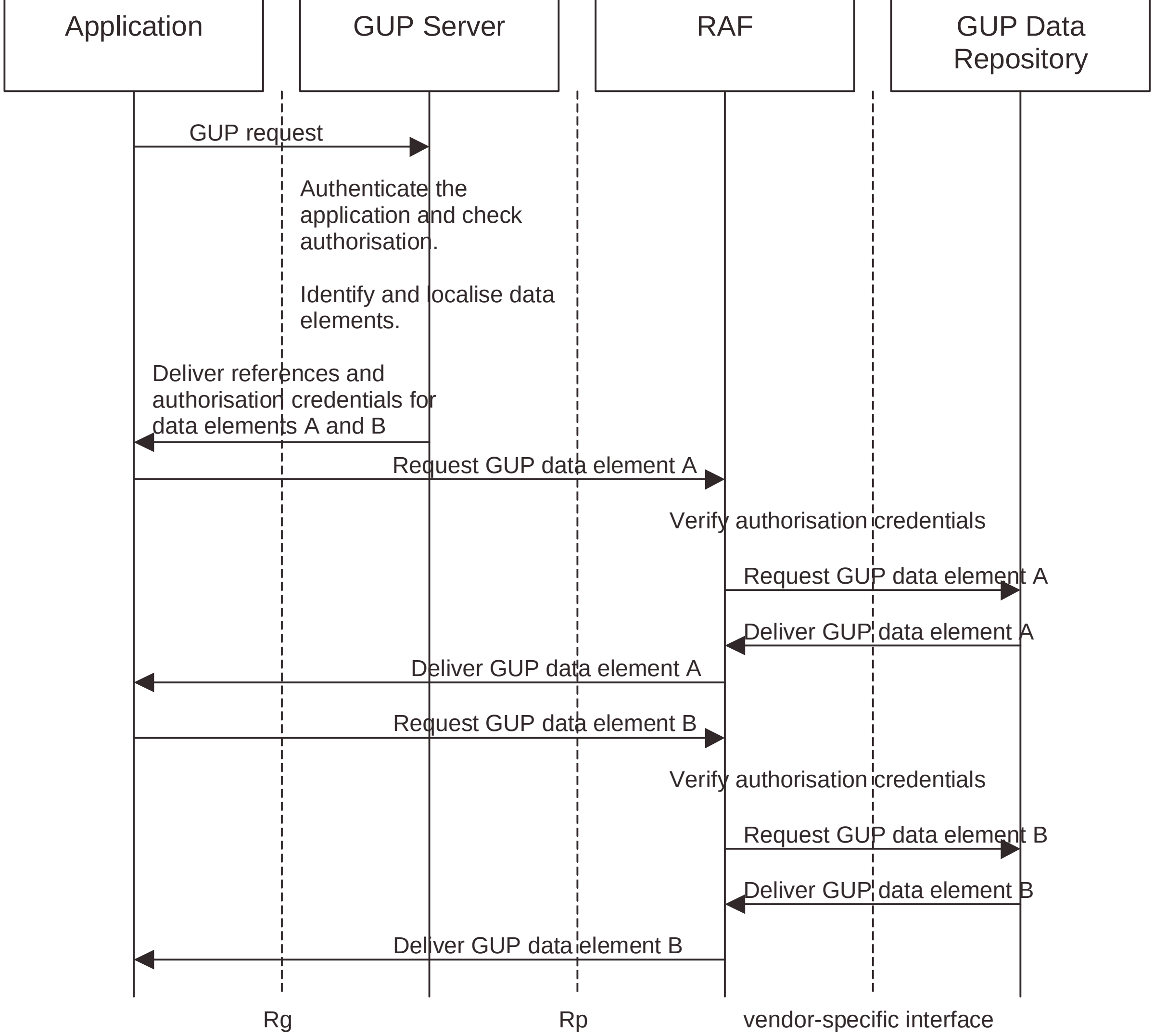

Application
GUP Server
RAF
GUP Data Repository
GUP request
Authenticate the application and check authorisation.
Identify and localise data elements.
Deliver references and authorisation credentials for data elements A and B
Request GUP data element A
Verify authorisation credentials
Request GUP data element A
Deliver GUP data element A
Deliver GUP data element A
Request GUP data element B
Verify authorisation credentials
Request GUP data element B
Deliver GUP data element B
Deliver GUP data element B
Rg
Rp
vendor-specific interface

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