3GPP TS 22.240 V11.0.0 (2012-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Service requirements for
3GPP Generic User Profile (GUP);
Stage 1
(Release 11)

Keywords
LTE, UMTS, user

3GPP

Postal address

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

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, e.g. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document introduces the requirements and features of a 3GPP Generic User Profile (GUP). The GUP will help overcome some of the challenges associated with the introduction of sophisticated user terminals with widely varying capabilities, hybrid combinations of mobile network domains, the advent of downloadable applications, and the desire of users to customise potentially complex services to individual preferences and needs.

The present document for a Generic User Profile will capture requirements that will allow:

1. A way to express user preferences in a consistent manner.
2. Effective management, control ownership and protection of GUP data.
3. Extensibility to cater for future needs and the simple addition of new features.

1. Scope

The present document defines the stage one description to the 3GPP Generic User Profile (GUP). It specifies requirements to the 3GPP Generic User Profile, seen primarily from the user, home environment, serving network and value added service provider's points of view.

The present document includes information applicable to the home environment, device- and network manufacturers and value added service providers which are sufficient to provide complete support of services in 3GPP networks.

While the 3GPP Generic User Profile may contain components that are out of scope of 3GPP (e.g. for services offered by third parties) the requirements in the present document pertain only to those components that lie within the 3GPP system.

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 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 32.140: "Subscription Management Requirements".

[3] Open Mobile Alliance (OMA): OMA-RD-Parlay_Service_Access-V1_0-20100427-A.

[4] W3C Recommendation "Extensible Markup Language (XML) 1.0" http://www.w3.org/TR/REC-xml

[5] W3C Recommendation "XML Schemas, Part 1: Structures" http://www.w3.org/TR/xmlschema-1/

[6] W3C Recommendation "XML Schemas, Part 2: Datatypes" http://www.w3.org/TR/xmlschema-2/

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and 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. The Generic User Profile is defined using the W3C XML recommendation [4].

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

GUP Component instance (physical): a GUP component instance is a physical representation of a GUP component. To one GUP component (logical) correspond one or more component instances, i.e. physical copies. Component instances may be located in the Home Network, in the Value Added Service Provider Environment and/or the User Equipment.

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

GUP Data Model: The data model describing the data structure, the way the data elements are defined and the relationship to each other.

Data Description Method: A method describing how to define the data contained in the Generic User Profile. The description is defined using the W3C XML Schemas recommendations [5], [6].

Master component instance (aka master instance): Among the component instances (physical) associated with a GUP component (logical), one of them is tagged with the role of "master instance". The master component instance is responsible for the correct value of the corresponding GUP component.

Public User Identity: Identity which is used to communicate with other users.

User: for definition see 3GPP TR 21.905 [1]. In addition the present document assumes, that the user has a unique identity in the 3GPP system (IMSI or IMS Private ID) and is associated with one 3GPP subscriber. (Note, that a user may have many addresses though! E.g. the user can have several Public User IDs). The user is not necessarily identical to the 3GPP subscriber.

Further 3GPP system related definitions are given in 3GPP TR 21.905 [1].

3.2 Abbreviations

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

GERAN	GSM/EDGE Radio Access Network
GUP	3GPP Generic User Profile
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
MVNO	Mobile Virtual Network Operator
OSA	Open Service Access
PID	Private User Identity
UE	User Equipment
UTRAN	Universal Terrestrial Radio Access Network
VASP	Value Added Service Provider
VHE	Virtual Home Environment
WLAN	Wireless Local Area Network

Further 3GPP system related abbreviations are given in 3GPP TR 21.905 [1].

4 General description

4.1 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 means to enable harmonised usage of the user-related information originating from different entities. The specification of the GUP shall also allow extensibility to cater for future developments.

The 3GPP Generic User Profile is the collection of User-related data which affects the way in which an individual user experiences services where a community of entities share this data. The 3GPP Generic User Profile can be stored in the home network environment and/or Value Added Service Provider equipment.

The 3GPP Generic User Profile will be accessed by different stakeholders and managed either by one (centralised) or by different stakeholders (de-centralised) such as the user, subscriber, value added service provider and network operator by a standardised access mechanism. The 3GPP Generic User Profile allows intra-network usage (i.e. data

exchange between applications within a mobile operator's network) and inter-network usage (between mobile operator's network and value added service providers) as illustrated in Figure 1.

NOTE: MVNOs and visited networks are treated as value added service providers in terms of GUP data exchanges with mobile operator's network.

The 3GPP Generic User Profile may be also be used by different applications in a standardised way.

The 3GPP Generic User Profile will help to create and manage the user data in each entity and on the other hand to make it easier to find all user related data as a whole in the home network environment.

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

4.1.1 Intended Usage of the Generic User Profile

The intended usage of the 3GPP generic user profile is a critical factor driving its detailed specification, e.g., architecture and data model. In general, user profile data can be shared between different stakeholders to facilitate the following:

- **User preference management**: Enable applications to read and utilize a limited set of user preference information
- **User service customization**: Enable applications to read and utilize personalized service information, i.e., individual settings for a particular service
- **Terminal capability management**: Enable applications to access terminal-related capabilities
- **User Information sharing**: Enable applications to read and utilize application level information, e.g. address book information
- **Profile key access**: Enable applications to use a unique identity as a key to access profile information, .e.g. any public user identity or an alias.

It is intended that the 3GPP GUP, in particular, will address all of the above. As can be inferred, a user's identity can serve as the unique common key into the profile.

4.1.2 Benefits of the 3GPP Generic User Profile for individual stakeholders

The following chapter shows in an exemplary way how stakeholders may benefit from GUP. The examples given are neither exhaustive nor are they meant to be part of, or be implemented by GUP. On the contrary, these functions / use-cases need to be seen distinct from GUP, but capabilities offered through GUP (e.g. a common data description, data access- and synchronisation mechanisms …) may be utilised to build these functions.

- Subscription Management and Customer Care:
  Subscription Management [2] benefits from a standardised way to access subscription data of a user. Already today customer care is a noticeable part of an operator's expenses, it will grow to be even more expensive as more services and more terminal types become available for 3GPP system. Unlike the Supplementary services in GSM new services in 3GPP are not standardised. Therefore content and format of subscription data as well as the places (repositories) where subscription data are stored may be different for different new services. GUP specifies the description of- and access of data in a standardised way. This will allow:
  - **Service providers** as well as Value Added Service providers to use standardised GUP mechanisms for Subscription Management and Customer Care by the operator.
  - Reduce costs for Subscription Management and Customer Care for the **operator** and/or **service provider** and/or value added service provider since management tools may rely on this standardised mechanism.
- Subscription Check by third party provided services:
  Third party provided services may run on application servers outside the 3GPP system. However subscription information may be kept by the home operator.

To find out, whether a service is allowed to be invoked by a particular user the service needs to check its subscription. Access to this information can be controlled by means of GUP mechanisms.

- Benefit for third party **value added service providers** and for
- **Operators**, who want to keep subscription within their domain

- Services Interaction:
  If personalisation of services possibly effect other services it may be advantageous, that such personalisation is visible to these other services. If a service is designed to permit access to these data through GUP mechanisms:
  - the **user** or **operator** may choose to allow certain services to access certain user data of other services of the user.

- Provision of Terminal Capability information:
  Services (from the home- or visited network operator or provided by third parties) may need to know what capabilities the terminal, that is currently used by the user, supports. Multiple provisioning protocols are a problem for terminal vendors since the UE has to support all of them. The GUP data will be described in the same way and can therefore be used in different protocols without having to change. GUP mechanisms could provide the basis for retrieval of a user's terminal capabilities.
  - Benefit for the **value added service provider**, who can rely on a GUP mechanism to obtain this information.

4.2 Conceptual view of the GUP

For each user (characterised by an IMSI or IMS PID) one User Profile exists, which may consist of several 'components'. These components may be distributed in the home network and value added service provider's environment. Within the home network, the components may be distributed in various network nodes. Figure 1 below provides a conceptual overview of GUP and is as such for informative purposes only. Only one master of the component exists, but one or more copies of the master component may exist. The home operator shall be able to copy master components, which are located outside the home network to the home network. Within the home network, functionality exists that is able to locate GUP components, thereby making applications unaware of the actual location of the components. The administration and management of the data associated with this functionality is under the control of the home network. Although GUP does not attempt to provide an actual classification of the data it may contain, one may consider categorisations such as general user information, terminal related information, service specific information, etc. as indicated in subclause 4.4.

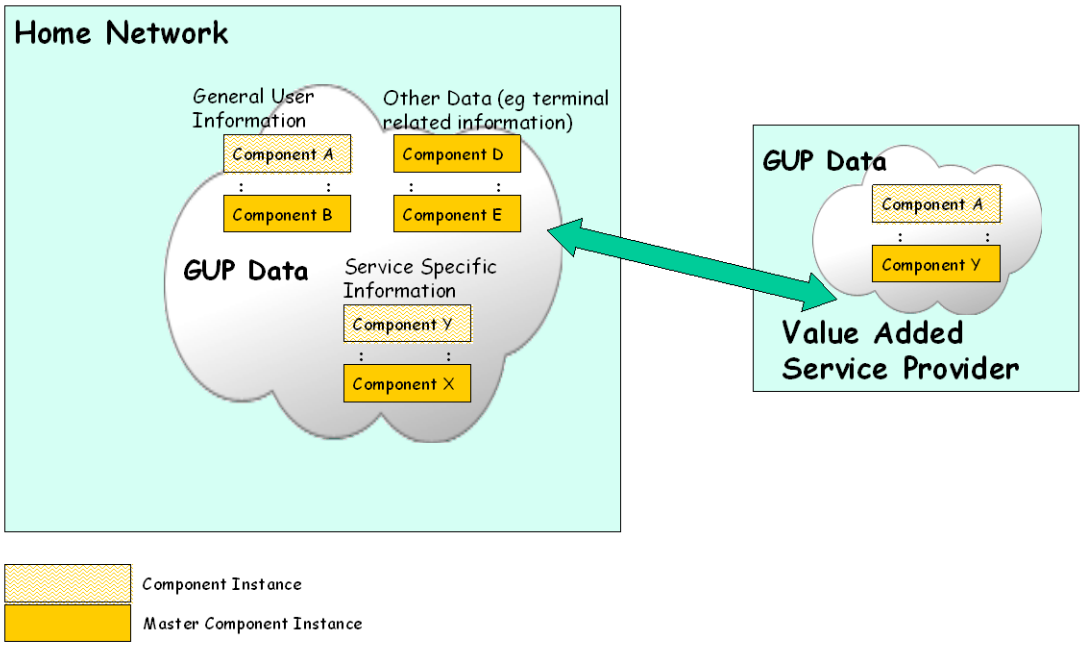

Figure 1: Conceptual view of GUP

4.3 GUP Data Stores and GUP data Users

This subclause describes in general terms where the generic user profile data resides and which entities use that information. A general feature of the user profile is that the different entities are data consumers for a certain subset of the generic user profile and are data suppliers for another part. The 3GPP GUP data are distributed by nature and consequently stored in home network and Value Added Service Provider Equipment.

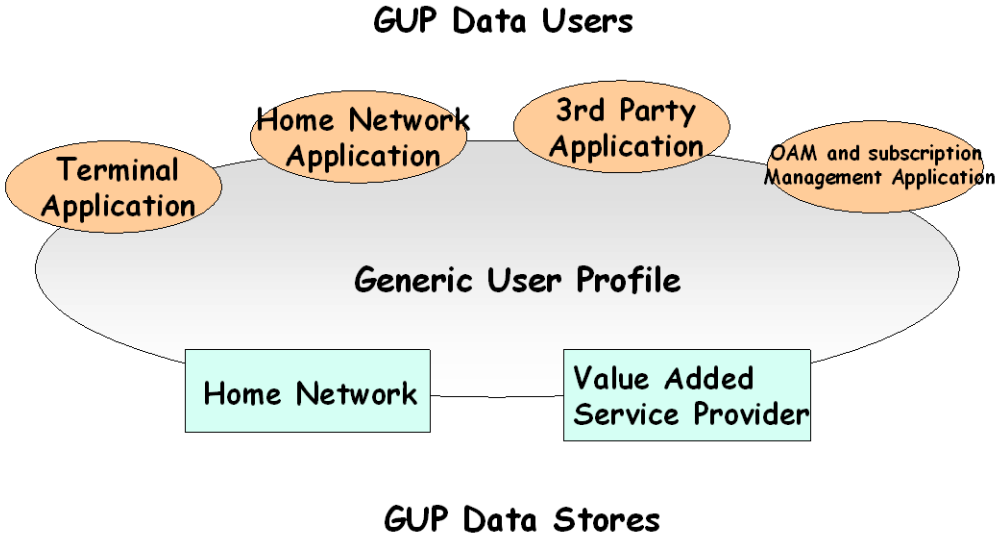

Figure 2: Illustration of the scope of 3GPP Generic User Profile

The Generic User Profile provides a generic mechanism to access and manipulate user related data for suppliers and consumers. Using this mechanism the data can be retrieved and managed in a uniform way. However the data contents itself are not described within the Generic User Profile, but only the data model and a schema shall be defined.

The suppliers and consumers of the data can be divided into the following groups of applications:

- Applications in the home network
- 3rd Party Applications
- OAM and subscription management applications

Applications in the home network may include those related to call or session handling as well as messaging or web services. Typically fairly high requirements are set on the response time.

3rd Party Applications are similar to applications in the home network but they are non-trusted which means that strict security, access and privacy procedures shall be carried out.

OAM activities related to user profile are provisioning and administration of user data by the network operator. These activities are characterised by needs for high throughput and allow longer response time. In order to allow simple and centralized administration it should be transparent to the administrator where the different parts of the user data are stored. As a result, this role needs a single system image on user profile, or, on functional terms, a common data access function. As one alternative the user self-service management may be implemented as part of this function.

4.4 Synchronisation model

GUP components instances may be distributed in the home network and value added service provider's environment. The distribution model is shown in Figure 1.

A data consumer can request a copy of a GUP component, i.e. the master instance of the component. This copy may be a **working copy** or a **synchronised copy**.

Master instance: the data supplier holds the master instance of a GUP component.

NOTE: During the lifetime of a component, the role of *master instance* may be played by different component instances (e.g. in the case of failure). But at any point in time, there is always one and only one "master instance". This implementation aspect is beyond the scope of GUP.

A ***synchronized copy*** of a GUP component is a component instance that is kept synchronized with the master instance.

Synchronization here means that changes made to the master instance will be propagated to the synchronized copy (e.g. update, deletion, etc.) The synchronized copy is held within the data consumer's local store..

A ***working copy*** of a GUP component is a component instance that corresponds to a copy (or snapshot) of the master instance at a given point in time. The working copy is held within the data consumer's local store. Future changes to the master instance (e.g. update, deletion, etc.) are NOT propagated to the working copy. The working copy remains unaffected by changes of the master instance of the GUP component.

If a GUP component is no longer applicable for a given user, the master instance for this GUP component is deleted and all data stores holding synchronized copies are notified about this deletion.

If the access rights of the component are changed, a proper notification is sent to the owner of the synchronized copy.

4.5 Contents of GUP

The present document does not mandate any data to be part of the 3GPP Generic User Profile. However the following kind of data are considered to be useful for inclusion in GUP.

1. Authorised and subscribed services information:

These kind of data are generally owned by the home operator and allow management and interrogation of subscription information and would typically consist of:

- authorised services that the subscriber may subscribe to
- services the subscriber actually has subscribed to

2. General user information

Data, owned by the user, which are not specific to individual services, but may be useful for any service. These would be data like

- settings (e.g. name, postal address), preferences (e.g. language)
- Registered Service Profiles of the user, indicating the currently active Service Profile of the user.

3. PLMN specific user information

Data, owned by the home operator, which are not specific to individual services, but may be useful for any service. These typically would be data like

- addresses (e.g. MSISDNs, URLs) of the user.
- WAP parameters (e.g. standard WAP gateway)
- GPRS parameters (in UE and HSS)
- Preferred access technologies (The preferred access technology, second preferred access technology etc. e.g. UTRAN, GERAN, WLAN etc.)

4. Privacy control data of the user

Data, owned by the user, which are specific to individual services and which control privacy settings of that service. These could e.g. be

- Privacy settings for standardised services like the Presence service or Push service.
- Privacy settings of non-standardised services.

5. Service specific information of the user:

Data, owned by the user or value added service provider, which are specific to individual services (standardised or non-standardised). These could e.g. be

- Service customisation data of the user.
- Service authentication- and authorisation data (for "single sign on") like keys, certificates, passwords...

6. Terminal related data

These are data, which relate in particular to the user's terminals (ME and UICC). These could e.g. consist of

- Terminal capabilities of the terminal currently in use (e.g. User Interface capabilities, communication capabilities, available services, service capabilities,…).
- Data for initial configuration and/or reset of the ME.
- Backup data for recovery of the ME configuration including service specific data.

7. Charging and billing related data

This data consists of information necessary for the user related charging and billing. This data could e.g. consist of:

- The billing policy

NOTE: The following data categories are not considered to be useful for the 3GPP Generic User Profile:

- Run Time Data.
  Data that are created during the initiation of the session, call or application execution and if they are only available during the lifetime of such session, call or application execution then they are considered as Run Time data.
- Historic/Statistic Data.
  User/system behaviour information (e.g. statistics on the usage preferred web pages; duration, number of calls, error rate).

4.6 The role of Data Description in GUP

GUP provides a means of supporting access to data for ranges of services and functions (e.g. MMS, Presence). The support of users' services and personalization data may result in manipulating data in a structured manner, and a standardised way of describing and accessing these data structures, utilizing a Data Description Method based on XML Schema.

As there may be technologies which have impact on the GUP but could not be included in the Data Description Method, the Data Description Method should take this coexistence with other technologies into consideration.

5 Stakeholder requirements

These requirements are given from the perspective of the key stakeholders.

The stakeholders within the context of GUP are:

- the Subscriber

NOTE: The subscriber may hold subscriptions for one user (e.g. in the case the subscriber is identical with the user) or several users (e.g. in the case of a company - the subscriber – holding subscriptions for it's employees – the users)

- the User

NOTE: The user may or may not be identical with the Subscriber.

- the Value Added Service Provider
- the Home Network Operator
- the Roamed-to Network Operator
- the Regulator

5.1 Subscriber Requirements

For a subscriber's services, that support and are supported by GUP:

- The subscriber shall be able to customise her subscribed services and interrogate customisation settings, subject to limitations by the Home operator and/or value added service provider. The user interface for customisation/interrogation is service specific and out of scope of this specification.

5.1.1 User Requirements

For a user's services, that support and are supported by GUP:

- The user shall be able to customise the services , that have been subscribed to her by the subscriber and interrogate customisation settings, subject to limitations by the Home operator and/or value added service provider and/or subscriber. The user interface for customisation/interrogation is service specific and out of scope of this specification.

5.2 Value Added Service Provider Requirements

VASP services, i.e. services provided by Value Added Service Providers (VASP), shall – via mechanisms of the GUP – be able to:

- Identify the network, the service and the user in any GUP related operation
- Check a user's subscription information for the service.
- Provide access to a user's service specific GUP data stored by the application (according to the access rights set by the user).
- Access other GUP data of the user subject to limitations of access rights

VASP services – standardised and non-standardised – may be part of the 3GPP system (as operator supplied services in the home-network or in a different 3GPP network) or may reside outside the 3GPP system.

It shall be possible for VASP services outside the 3GPP domain to access GUP only via a secure interface to the 3GPP system.

5.3 Home Network Operator Requirements

The home network operator shall, via GUP mechanisms, be able to:

- support On-line Service Registration

  Subscriber service registration can be set up by on-line subscription not just by customer care. This will also reduce Customer Relationship Management (CRM) workload.

- access Terminal Capabilities

  Terminal capabilities (e.g. software and hardware information, application features, etc) shall be accessible to the network. This information may be used to enable any services within network.

- access Value Added Service Provider Capability Information

  Value Added Service Provider capability information (e.g. Compression algorithms, Billing capabilities) should be accessible to the network. This information may be used to provide end-to-end service according to UE, Network and the Value Added Service Provider's capabilities.

5.4 Roamed-to Network Operator Requirements

None yet identified.

5.5 Regulatory Requirements

None identified in addition to the considerations in clause 8. Privacy and Authorisation.

6 General Requirements

This clause includes different general technical requirements which are not from the perspective of a particular stakeholder.

6.1 Network Requirements

These requirements are collected from the point of view of technical Network infrastructure and Elements:

- The GUP data shall be accessed by standardised GUP interfaces and protocols which use the generic GUP data model to carry the user profile.
- The GUP Interface shall be independent of the structure and semantics of the data.
- The GUP access mechanism shall support accessing of the whole profile data or a selected part of it.
- The GUP access mechanism shall include read, create, modify and delete access. GUP shall provide these access mechanisms to read, create, modify, and delete data of GUP components.

Note: This does not include installation and modification of the structure of GUP components at a specified data store, nor does it imply management of GUP data stores of GUP component instances.

- The GUP data shall be transferred in a standardised way.
- The GUP interface shall include a standardised way for access control.
- The GUP interface shall enforce the subscriber privacy.
- The GUP interface shall enforce the user privacy.
- The GUP shall not cause significant additional load or delays to the network functions and elements.

6.2 UE Requirements

This subclause includes different UE specific requirements for the 3GPP GUP.

- GUP shall provide mechanisms torepresentUEdata as GUP components in the network(e.g. terminal capabilities, user preferences, etc).
- Network based applications should have "read" access to GUP components representing UE data, irrespective of the connection status of the UE.
- It shall be possible to back up GUP data to the home network or VASP network and to restore it to a UE, however, the mechanism used is outside the scope of GUP.

6.3 General Service Requirements

This subclause includes different Service aspects and requirements for the 3GPP Generic User Profile. The following general requirements from the point of view of different Service Applications apply:

- It shall be possible for an application to retrieve the whole user profile or selected parts of it in one transaction.
- There shall be effective means to retrieve individual GUP data elements with acceptable delay for real-time services.

One typical use case for the latter requirement is a call control application that would take advantage of subscriber's preferences or charging related information.

Third party applications may take advantage of the features specified e.g. for Open Service Access (see 3GPP TS 22.127 [3]) to access GUP data.

The description of GUP data shall be easily extensible for new, proprietary uses without any problems caused for the existing or standard applications.

6.4 Management Requirements

This subclause includes different technical Management aspects for the 3GPP Generic User Profile based on the needs of e.g. Self-Service Management, Subscription Management, Service Management, Network Element Management, Network Management and Customer Relationship Management.

In 3G networks it is expected that user profile data is not only distributed over different network elements but belongs to different administrative domains. These administrative domains may be closed against external access. However, in order to enable a seamless service experience for the user a controlled transparency to exchange user profile data is needed.

There exist two main cases to be addressed:

Domain borders in the home network:

Already in the network of the subscriber's home network operator there may exist different domains. Potential examples are application of 3rd party value added service providers which are loosely coupled with the network provider, e.g. their applications run under the brand of the network operator but their data are stored and maintained apart from the network operator's entities.

Domain borders between different network operators:

This is the well-known roaming scenario where a user is served by another network than his home one. Roaming is already addressed by mobile networks but in the case of 3G networks there is an important additional requirement: The assumed frequent changes of applications induces a need to handle frequent changes of data sources/consumers.

The user profile data access architecture shall enable the transparent and flexible usage of the user profile data. It shall provide transparent access to distributed data fulfilling the needs of the different roles described above. Furthermore, the architecture shall address the fact that parts of the user profile data are potentially located in different administrative domains. Possible means are negotiation capabilities and proxy functionality at the domain borders.

Management of GUP data components:

Making a particular data store available for GUP is not in the scope of GUP and needs to be administered by other means.

The administration (installation and modification) of the structure of GUP components at a specified data store is not in the scope of GUP and needs to be administered by other means.

6.5 Synchronization Requirements

To avoid unnecessary duplicated data storage an application should be able to access parts of the user's GUP data.

The following requirements are applicable to the synchronization model:

1. GUP shall offer a mechanism to define *synchronized copies*, i.e. instances that are kept synchronized with the master instance.

2. GUP shall offer a mechanism to define *working copies*, i.e. instances that do not require any synchronization.

3. GUP shall make sure that synchronized copies do not conflict with the access right of the corresponding GUP components. For example, if the access rights to some parts of the GUP component change such that the data consumer no longer has access rights, then those parts of the GUP component would no longer be synchronised.

6.6 Data Description Requirements

The Generic User Profile is a generic, extensible profile data collection with mechanisms to e.g. create, retrieve, delete and modify the data. GUP shall define a standardised way of data description. This allows for a standardised access and handling of these data, not excluding the possibility of proprietary extensions.

Only part of the data contents are standardised within 3GPP specifications, whereas application specific data is outside the scope of the 3GPP standardisation. This specification does not mandate any 3GPP service specific data to be part of the 3GPP Generic User Profile. However the common data types shall be specified to facilitate the separate work on the service specific definitions (e.g. for the user profile in HSS).

The common data shall contain data types for at least:

- Private IDs (IMSI and IMS Private User Identity)
- Public IDs (MSISDN and SIP URL)
- Other address types, that are supported by 3GPP (e.g. e-mail)
- Service identifications
- Generic privacy control data
- Date and time
- Service Subscription state (e.g. "active", "not subscribed", "dormant" ...)

7 Security

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

The secure mechanisms available shall include the following:

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

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

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

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

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

6. It shall be possible for the consumer of data to detect whether the data have been tampered with during transmission. .

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

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

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

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

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

8 Privacy and Authorisation

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

8.1 General Requirements

It shall be possible for the user to define privacy requirements for components of the 3GPP Generic User Profile to determine access rights.

It is agreed in the subscription agreement between the home network operator and the subscriber how the access and privacy control is carried out e.g. who is able to control different parts of the user profile including the privacy settings. The GUP shall provide means to implement access and privacy control according to the different agreements.

The GUP authorization shall be independent of who has set the privacy rules for each part of the GUP data. A generic mechanism shall be provided to ensure that only such data for which there is a valid authority can be created, read, modified or deleted.

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

8.2 Authorisation Rules

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

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

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

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

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

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

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

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

9 Charging

It shall be possible to support charging for the management, access and synchronization of the 3GPP Generic User Profile. (e.g. for capability negotiation or remote diagnostic information gathering).

NOTE: There might be legislative restrictions on charging. This is FFS.

Annex A (informative): Example 3GPP Generic User Profile use cases

1. Setting up a Subscription for a new customer

- Precondition
  - A person has just purchased a new device, and requires new subscription data to be initiated in the shop.
- Actions
  - Subscription data is input by the shop personnel by means of a Subscription Management application.
  - Subscription Management application stores the data in Generic User Profile in the Home Network.
- Post-condition
  - The user can leave the shop. Her subscription is ready to use.

2. Application Access to User Profile Data using OSA (Pull Scenario)

- Precondition
  - The application is registered with the OSA framework
  - The application is authorised to access the user profile management Service Control Function and use methods which permit read/write data in user profiles
- Actions
  - The application uses OSA to read/write data in the user profile of the user
  - The network provides the requested data or modifies the data as requested
- Post-condition
  - Consistency of the user profile data

3. Notification of user subscription to an HE-VASP application using OSA (Push Scenario)

- Precondition
  - The OSA application from the HE-VASP is registered with the OSA framework
  - The OSA application is authorized to receive subscription/unsubscription notifications
  - The OSA application has subscribed to the notification permitting to it to know when new users have subscribed to the service implemented by the OSA application
- Actions
  - A new user subscribes to the service implemented by the OSA application
  - The Home Environment notifies the OSA application about a new subscription and provides it with relevant information (e.g. identity of the user)
  - Possibly the OSA application provides the home environment with a link (e.g. URL) to a location where the user can customize the service

- Post-conditions
  - The OSA application can now have access to home environment -owned user profile information for this user, provided that it is granted the related access rights
  - The user can customize service data for the service implemented by the OSA application

4. Customization of service specific data for a VHE service provided by a HE-VASP

- Preconditions
  - The user has a VHE subscription
  - The user is subscribed to the service provided by the HE-VASP
  - There is a link from the user Personal Service Environment (PSE) to the HE-VASP for service customization
  - The user has access to her PSE and has successfully been logged to it
- Actions
  - The user accesses her PSE and decides to customize the service provided by the HE-VASP
  - She transparently access a service customization interface provided by the HE-VASP (possibly via a hyperlink)
  - She defines/modifies service customization data, which are managed and stored by the HE-VASP
- Post-condition
  - Next time she uses the service, new customization data will be used

Annex B (informative): Additional Information

Note: The following use cases are currently not in the scope of 3GPP Generic User Profile Stage 1 but they are still considered to be useful information (e.g. for future work) and therefore included in this Annex.

1. Setting up a Subscription for a new customer

- Precondition
  - A person has just purchased a new device, and requires a new subscription to be initiated in the shop.
- Actions
  - The user preferences for services are established.
  - Information about the terminal capabilities are received from the UE.
  - User Profile content is created for the Subscriber, and downloaded over the air, via local link or similar
- Post-condition
  - The user can leave the shop. Her phone/device is ready to use. Basic settings needed to start and run initial applications ready.

2. Initial Service Configuration (Bootstrap)

- Precondition
  - No settings made, user with a subscription
- Actions
  - Settings, partly based on user profile downloaded over the air, via local link or similar
  - The download initiated by the value added service provider, network operator, 3rd party or user
- User Data
  - Setting received could include basic connectivity configuration parameters and the user's security policy
- Post-condition
  - The user's phone/device ready to use. Basic settings needed to start and run initial applications ready

3. Backup/Restore of User Profile Components stored in the UE

- Precondition
- Backup
  - The phone is configured, all the user preferences are set.
  - The settings include user profile parameters such as generic parameters, service personalisation parameters, user's security policy and other user preferences
- Restore
  - The phone's initial configuration enables download of configuration and user data at least via local link.
  - A backup of phone configuration and user preferences is available in the network.

- Actions
  - The user wishes to backup or restore the current version, or parts of the current user profile to the network, or to another UE.
  - The backup/restore is performed via local link or remotely towards the network
  - The backup/restore can be initiated by the user, the value added service provider, 3rd parties or the network operator
- User Profile Storage
  - Secure area of the (U)SIM or ME or retained in the network by the value added service provider. User private data is only stored in the network with the user permission.

4. Content Negotiation

- Precondition
  - The user has set her preferences in the UE
  - Terminal type capability information is stored in ”internet”
- Actions
  - The user initiates request for content. The request contains:
    - User preference fetched from the UP
    - Reference to the capability information is stored in ”internet”
    - Deviating capability information
  - Returned content selected or tailored according to User preferences and capability information

5. Terminal Management – Manual Helpdesk

- Precondition
  - A user is complaining because her pocket web browser does not work. He calls the helpdesk
- Actions
  - The UE capabilities are established by the helpdesk person
  - A helpdesk person at an operator, value added service provider or enterprise verifies that the correct operating parameters are set on the device of a complaining user
- Post-condition
  - The user's is happy. The pocket web browser is running correctly

6. Terminal Management – Automated Self Fixing

- Precondition
  - A software agent on the user’s device identifies an error.
- Actions
  - It contacts the helpdesk software entity to fix the problem.
  - The UE capabilities are established by the automated self-fixing solution.

- The self-fixing solution correctly diagnoses the error and provisions a bug fix.

- Post-condition
  - The user's device software executes correctly (and is happy)

7. Automatic Access Selection based on preferred list

- Precondition
  - The UE shall be able to support automatic access technologies selection (i.e. without user intervention).
  - The user has set her preferences in the UE and enabled automatic access technologies selection.
  - A list of preferred access technologies capabilities information is stored in ”internet”
  - The access technologies are authorized.
- Actions
  - The user equipment initiates request for selected access technology. The request contains:
    - User preferences fetched from the UP
    - Reference to the access technology capabilities information is stored in ”internet”
  - The preferred access technology is selected.
- Post-condition
  - The preferred access technology is selected based on the order of precedence defined in a list of access technologies on the UE. The switch to a less preferred access technology, in case the most preferred is not available, takes place without user intervention.

8. Multiple Access Technology Negotiation

- Precondition
  - The user has set her preferences in the UE and enabled access selection.
  - Terminal type capability information is stored in ”internet”
  - The access technologies are authorized
  - The user has access and connection with one ongoing application
- Actions
  - The (Multi-mode) terminal initiates request for another access technologies.
  - The terminal chooses the most appropriate access form based on the UP and/or the sessions in progress demand of service quality.
  - Returned access form selected according to User preferences and capability information.
- Post-condition
  - Change of access technology without interrupting any session(s) to/from that host (context transfer).
  - The old access connection end.
  - The user and the terminal are connected via the new access (i.e. WLAN) with the same user identity, without having to re-authenticate.

Annex C (informative): Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

3GPP TS 21.133: "3G Security; Security Threats and Requirements".

3GPP TS 22.097: "Multiple Subscriber Profile (MSP) Phase 1; Service description - Stage 1".

3GPP TR 22.121: "The Virtual Home Environment".

Annex D (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-19	SP-030036		22.240			Rel-6		Approved at SA #19	2.0.0	6.0.0	
SP-21	SP-030469	S1-030965	22.240	001		Rel-6	F	Clarifications for section 7 of 22.240	6.0.0	6.1.0	GUP
SP-22	SP-030707	S1-031256	22.240	002	-	Rel-6	F	Clarifications on general service requirements and data description requirements	6.1.0	6.2.0	GUP
SP-22	SP-030707	S1-031257	22.240	003	-	Rel-6	F	Clarifications GUP data access and administration	6.1.0	6.2.0	GUP
SP-22	SP-030707	S1-031258	22.240	004	-	Rel-6	F	Clarifications on GUP synchronisation	6.1.0	6.2.0	GUP
SP-23	SP-040095	S1-040202	22.240	005	-	Rel-6	F	GUP UE Requirements	6.2.0	6.3.0	GUP
SP-25	SP-040507	S1-040683	22.240	006	-	Rel-6	F	GUP, UE requirements corrections	6.3.0	6.4.0	GUP
SP-26	SP-040730	S1-040989	22.240	007	-	Rel-6	F	Removal of erroneous use cases	6.4.0	6.5.0	GUP
SP-42						Rel-7		Upgraded to Rel-7 without technical change.	6.5.0	7.0.0	
SP-42						Rel-7		Upgraded to Rel-8 without technical change.	7.0.0	8.0.0	
SP-46	-	-	-	-	-	-	-	Updated to Rel-9 by MCC	8.0.0	9.0.0	
SP-49	SP-100575	S1-102054	22.240	0008	-	Rel-9	D	Removal of references to 3GPP OSA	9.0.0	9.1.0	TEI9
2011-03	-	-	-	-	-	-	-	Update to Rel-10 version (MCC)	9.1.0	10.0.0	
2012-09	-	-	-	-	-	-	-	Updated to Rel-11 by MCC	10.0.0	11.0.0	