3GPP TSG SA WG3 Security — S3#22 **S3-020124**

25 - 28 February 2002 Bristol, UK

3GPP TS 22.240 V0.6.0 (2002-02)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Stage 1 Service Requirement for the 3GPP Generic User Profile (GUP) (Release 6)

Keywords
<User, Profile>

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

Editor's note: The introduction should be reworked. The original introduction has been replaced with SA1-020076 with some rewording

This specification 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.

This specification for a Generic User Profile will capture requirements that will allow

1. A way to express user preferences in a consistent manner,
2. Distributed storage and efficient replication of data,
3. Effective management, control ownership and protection of data.
4. 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 service provider's points of view.

This TS includes information applicable to the home environment, device- and network manufacturers and 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 this specification 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: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications.

[2] 3GPP TS 22.121: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service Aspects; The Virtual Home Environment".

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

[4] 3G TS 21.133: "3G Security; Security Threats and Requirements".

3 Definitions, symbols and abbreviations

Here are only included definitions that are in addition to that in 21.905.

Editor'note: Definitions should be revised according to the content of the specification

3.1 Definitions

3GPP Generic User Profile: The 3GPP Generic User Profile is the collection of data which is stored and managed by different entities such as the UE, the Home Environment, the Serving Network and Value Added Service Provider, which affects the way in which an individual user experiences services.

Data Consumer*:* A data consumer is an entity which uses data stored and controlled by another network entity.

Data Source: A data source is an entity which stores and controls data relevant for its operation.

User Profile Component: User Profile components are all the detailed data that specifies: General user and subscriber info, UE and application capabilities, subscriber settings, user preferences, user settings, identifiers, security policies and settings, etc. A user may have zero, one or more instances (specific values) of a specific User Profile component, which is defined here as a logical grouping of related data. An instance of a User Profile component includes identity, type, structure, access rights, storage locations, and ownership.

3.2 Abbreviations

Here are only included definitions that are in addition to that in 21.905. For the purposes of the present document, the following abbreviations apply:

GUP 3GPP Generic User Profile

4 General description

[Editor's Note: Need to add further text]

This clause will include:

- primary reasons to specify the 3GPP Generic User Profile
- main advantages of the 3GPP Generic User Profile for different stakeholders such as Users, Subscribers, Service Providers, Network Operators and Manufacturers
- basic definition of the 3GPP Generic User Profile
- classification of the 3GPP Generic User Profile Data
- high level role of the 3GPP Generic User Profile from the point of view of the Network, Services and UE's

4.1 Introduction

The fact of having several domains within the 3GPP mobile system (e.g. Circuit-Switched, Packet-Switched, IP Multimedia Subsystem) 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 Service Providers to create, access and manage the user-related data located in different entities.

The objective of specifying the 3GPP Generic User Profile is to provide a conceptual description to enable harmonised usage of the User-related information located in different entities. 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 is stored in different entities such as UE, Home Network Environment and Value Added Service Provider equipment, and which affects the way in which an individual user experiences services.

The 3GPP Generic User Profile will be accessed and managed by different stakeholders such as the user, subscriber, service provider and network operator by a standardised access mechanism.

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 shall provide an architecture, data description and interface with mechanisms to handle the data.

4.2 Conceptual view of the GUP

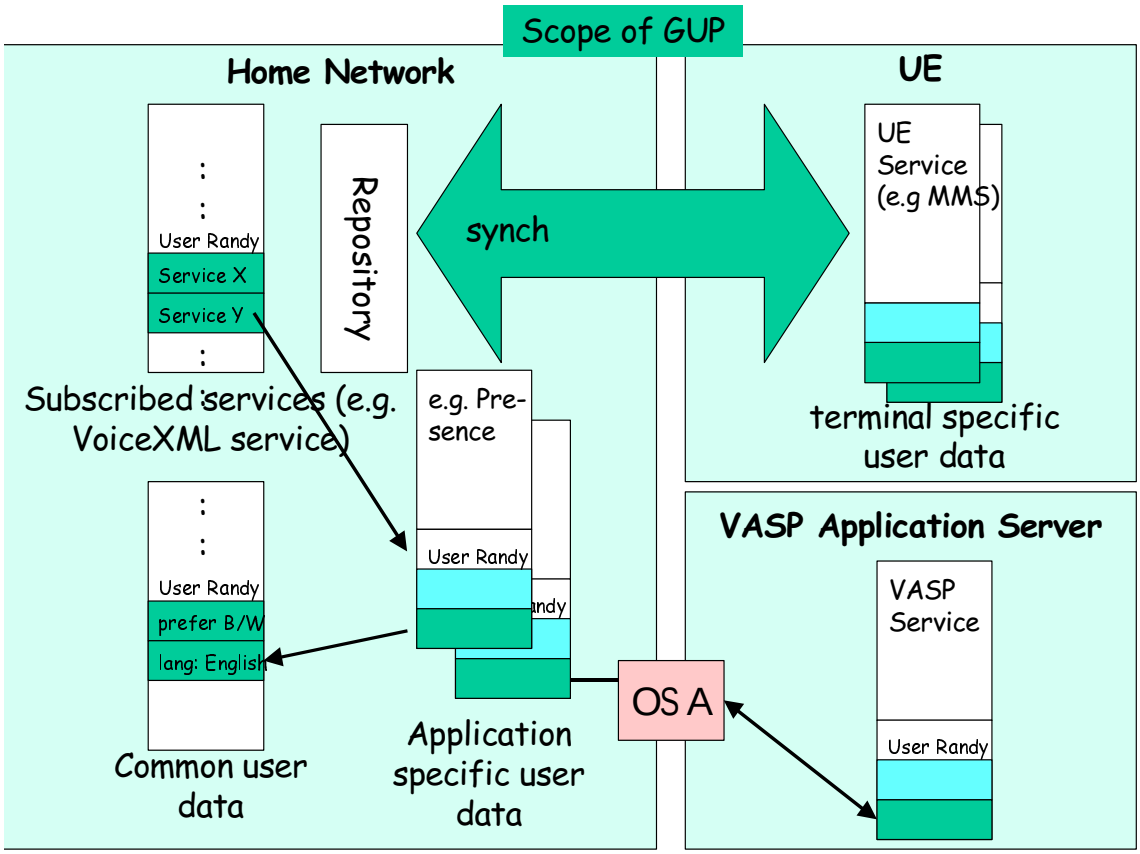
For each user (i.e. a 3GPP subscriber, characterised by an IMSI or IMS PID) one User Profile exists, but may consist of several 'components'. The following diagram provides a conceptual overview of GUP, and is for informative purposes only:

- A Value Added Service Provider may provide services which contain/provide user-related data. Some of the data will be generic, and stored as part of the GUP. Some data however will not be accessible to, or controlled by the GUP Service.
- In a similar fashion, a HE service may contain user data both generic and specific.
- There is a clear need for data synchronisation between the various data elements and repositories of GUP data.
- Although OSA is provided as an example of a 3GPP service interfaces, the diagram does not indicate a mandatory requirement for it to be supported in order to provide a GUP service.

Key

Green boxes indicate user data components accessible by GUP

Blue boxes indicate user data components which are non-accessible by GUP



An essential part of the GUP that is under control of the operator at least contains:

1. General subscription information of the user, consisting of

- a list of authorised services that the subscriber may subscribe to
- a list of the subscribed services (which can be used for subscription check) (these are the services the subscriber actually has subscribed to, a subset of the list of authorised services).

Note: Services that are outside the scope of 3GPP are outside the scope of this definition (e.g. user bookmarks, some VASP services). Complete visibility of all external services may not be provided.

2. Common user data

- Data which is not specific to individual services like addresses (e.g. MSISDNs), settings (e.g. privacy settings), preferences (e.g. language) e.t.c.

3. A repository for terminal capabilities and backup of terminal parts of the GUP.

- For recovery purposes GUP shall support a mechanism to allow applications in the terminal to keep a backup copy of parts of their user data in the network. However it shall be under the control of the user if such a backup copy is created and synchronised.

In addition one or more Service Profiles for a user may be supported. (e.g. for “business use”, “private”, “gone fishing” ...). A particular service may adapt service behaviour according to the currently active Service Profile of the user.

Application specific user data:

The user related data of services running on application servers (standardised or non-standardised) may be kept locally on these servers (without central management/control). The applications may want to make parts of the data available – e.g. for feature inte-rworking purposes – to other applications.

For this purpose the GUP shall define a mechanism that allows services running on application servers to make (parts of) their User data available as *external components* of the GUP in a standardised way.

Value Added Service Provider (VASP)

Some of these services may be even running on application servers outside of the 3GPP System. Access to those *external components* of the GUP may involve secure interfaces (e.g. OSA)

The GUP shall establish a standardised mechanism that allows applications to locate any (also external) components of the GUP. This standardised mechanism shall be under the control of the operator.

4.3 3GPP Generic User Profile Data Classification

[Editor's note: Need further discussion and verification of the following bullet points. Currently a lack of agreement on the definitions.]

The purpose of this classification is to understand the 3GPP Generic User Profile from a contents perspective i.e. what is within the scope of the 3GPP Generic User Profile.

The data that constitutes the 3GPP Generic User Profile can be classified according to the following classification criteria. This section contains a non-exhaustive list of classification criteria: Information Characteristics and Ownership. For each criterion there are examples.

Examples of data categories that are not part of 3GPP Generic User Profile

- Run Time Data. The data that is 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 call; error rate).

(a) Information Characteristics:

- **General Information**
  - General User Information (Name, address, age, sex, ID)
  - Logical identifiers (e.g. logical name, personal number, e-mail address)
  - General Subscriber Information (Name, bill info, users)
  - General Privacy preferences

- **Capability description**
  Describes the capacity of something. It is normally not configurable by the user. Capability information can be used to select the best content/information/function/strategy among a number of possible ones.
  - Terminal Capabilities
    As the number and variety of devices grows, there is a corresponding increase in the need to adopt the interaction depending on the capabilities of different devices. The terminal capabilities have to be described. Examples of terminal capabilities are: User interface capabilities, Communication capabilities, Synchronisation capabilities, MExE capabilities, WAP Browser capabilities.
  - Subscribed Network capabilities
    the variety of subscribed network capabilities will vary from user to user. There will be a need to describe the subscribed capabilities. Based on this information the subscriber will be allowed to gain access to the set of subscribed capabilities.

  [Editor's note: revisit the definition "service provisioning data" in previous draft]

  - Roamed-to Network Capability
    The capabilities of the used network will vary between networks and even within a network. The mobile environment related capabilities could differ from place to place. There will be a need to describe the supported capabilities. Based on this information and information about subscribed capabilities, the user will be allowed to gain access to the set of subscribed and supported network capabilities.
  - Subscribed Service Capabilities
    These data that provisioned to a user or not

- **User's Preferences**
  These are wishes set by the user, and indicate a preference to use one particular type of

content/information/function/strategy over another. A preference can be defined before you know which function will be using them. Examples are:

- User Interface preferences
- Browser appearance (User's preference for displaying frames)
- Preferred memory usage

[Editor's note: Need to revisit Service Customisation terminology and its relationship to capability description - above]

- **Service Customisation**
  This is information used to customise one or more services/applications/functions according to the user. Examples are:
  - User interface (Ring volume, Vibrating alert, Ring signals, Melodies, Key sound)
  - WAP Parameters (Bookmarks; Gateway: Internet account, Gateway IP address, User ID, Password, Data mode, Security, Show images, Response timer)
  - User security policy (application download, ciphering, positioning)
  - User Security data (Secret keys, user name)
  - Authentication data (e.g. password, pin, voiceprint)
  - Supplementary Services settings
  - Quality of service associated to the user
  - Status of Services (Active/deactive)

(b) Ownership:

The ownership of data is used in the access control. An entity does not automatically own the data stored in it. A trusted entity can store data owned by many different owners.

- **User**
- **Subscriber**
- **Home Network operator**
- **HE Value Added Service Provider**

[Editor's note: We need to revisit this bullet, regarding HE-VASP and VASP, and for Valued Application Service Provider – need to clarify definition. For both ownership and storage location]

4.3 Data Suppliers, Stores and Consumers

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 network entities are data consumers for a certain subset of the user profile and are data suppliers for another part. As a result, the user profile is a highly distributed data set across different network elements, terminals and administrative domains.

The figure 1 below shows the entities involved in handling of the 3GPP Generic User Profile.

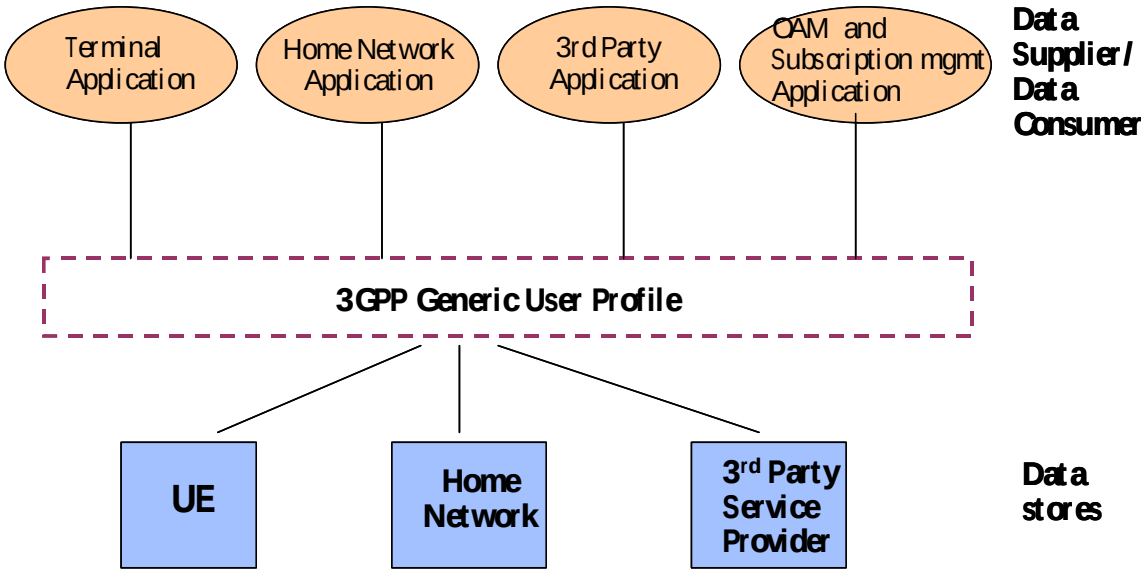


Figure 1. Illustration of the 3GPP Generic User Profile environment

The 3GPP Generic User Profile data may be stored in:

- UE
- Home Network
- 3rd Party Service Provider domain

The Generic User Profile provides a generic interface to the user related data for suppliers and consumers. Using this interface 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 shall be defined.

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

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

Terminal applications are of various nature and they can both supply Generic User Profile data to the above listed data stores and retrieve the data for use in the application. The real-time response requirements for the applications vary depending on the type of the application.

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 subscriber data by the network operator. These activities are characterised by needs for high throughput and longer response time. In order to allow simple and centralized administration it should be transparent to the administrator where the different parts of the subscriber 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.

5 Stakeholder requirements

[Editor's note: Specific requirements within Sections 5-9 are enumerated to help identify main isssue. The numbering of requirements does not represent any order of priority however]

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

5.1 Subscriber Requirements

5.1.1 User Requirements

1. The 3GPP Generic User Profile shall be available globally when roaming.

[Editor's note: This is a clear requirement, but has no agreed home]

5.2 Service Provider Requirements

This subclause will cover different type of service providers such as VASPs in Home Network, VASPs in other operators' Network and 3rd Party Service Providers.

5.3 Home Network Operator Requirements

5.5 Roamed-to Network Operator Requirements

5.6 Regulatory Requirements

Editor' note There are some regulatory considerations under 8 Privacy, does something else need to be considered here?

6 General Requirements

This subclause 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 3GPP GUP data shall be accessed by a standardised 3GPP GUP Interface and Protocol.
- The 3GPP GUP Interface shall be independent of the structure and semantics of the data.
- The 3GPP GUP access mechanism shall support accessing of the whole profile data or a limited part of it.
- The 3GPP GUP access mechanism shall include read, create, modify and delete access.
- The 3GPP GUP data shall be transferred in a standardised way.
- The 3GPP GUP interface shall include a standardised way for access control.
- The 3GPP GUP interface shall enforce the subscriber privacy.
- The 3GPP GUP shall not cause significant additional load or delays to the network functions and elements.

6.2 UE Requirements

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

6.3 General Application Service Requirements

This subclause includes different Service aspects and requirements for the 3GPP Generic User Profile such as requirements from the point of view of different Service Applications.

1. Where the full capabilities of the 3GPP Generic User Profile are not available because of failure of an entity or human error – the User shall experience a graceful degradation of service behaviour.

6.4 Management Requirements

This subclause will include different technical Management aspects for the 3GPP Generic User Profile based on the needs of e.g. Self-Service Management, Subscription Management, Service Management, UE 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 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.

1. 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.

7 Security

1. Secure mechanisms shall be available for the transfer of User Profile data to, from or between authorised entities.

2. Access to User Profile data shall only be permitted in an authorised and secure manner.

3. 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.

4. 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:

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

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

7. 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.

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

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

10. 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.

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

12. 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

13. User profile data in general is proprietary data owned by some companies. These data may not be exposed to everyone and not for free. *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.

14. 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 minimize the risk.

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

8 Privacy

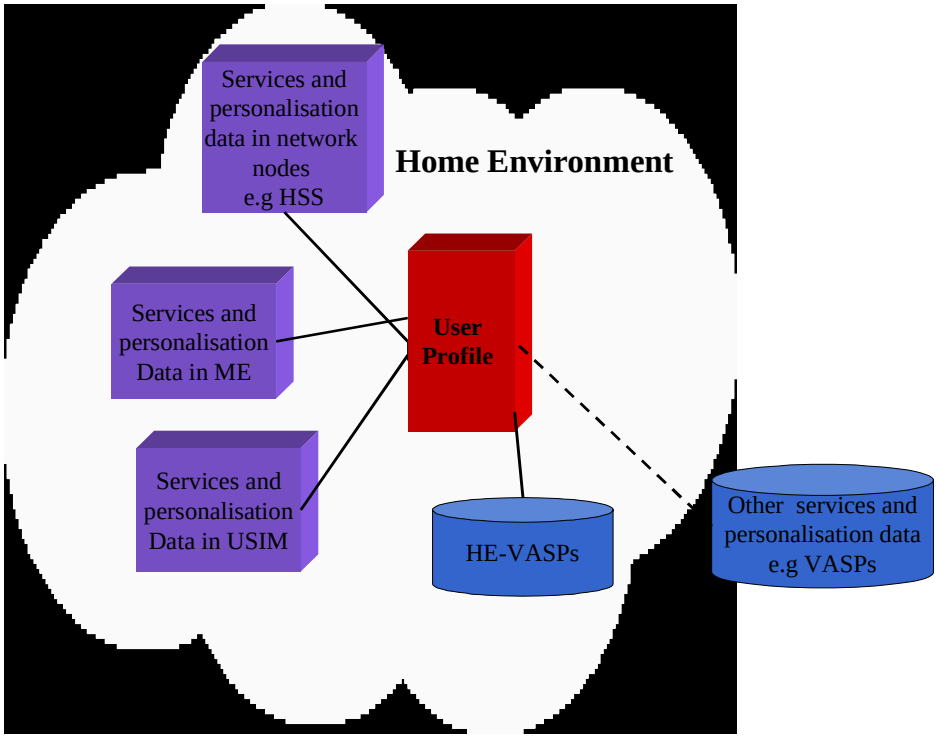
1. It shall be possible for the user to define privacy requirements for components of the 3GPP Generic User Profile to determine access rights. The privacy requirements shall fulfill local privacy regulations.

9 Charging

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

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

[Editor's Note: The following diagrams are for informative purposes. They present examples of the distributed locations of the User Profile components, location and related functions, as an aid for illustrating the listed use cases.]



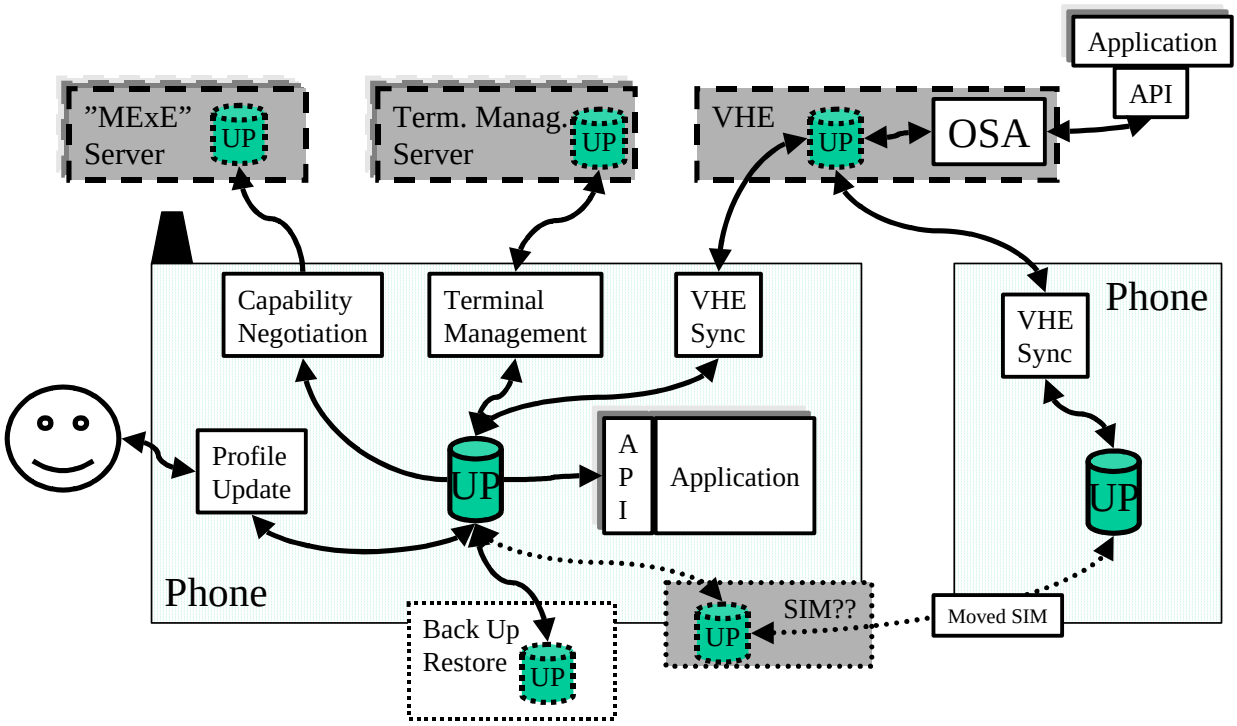
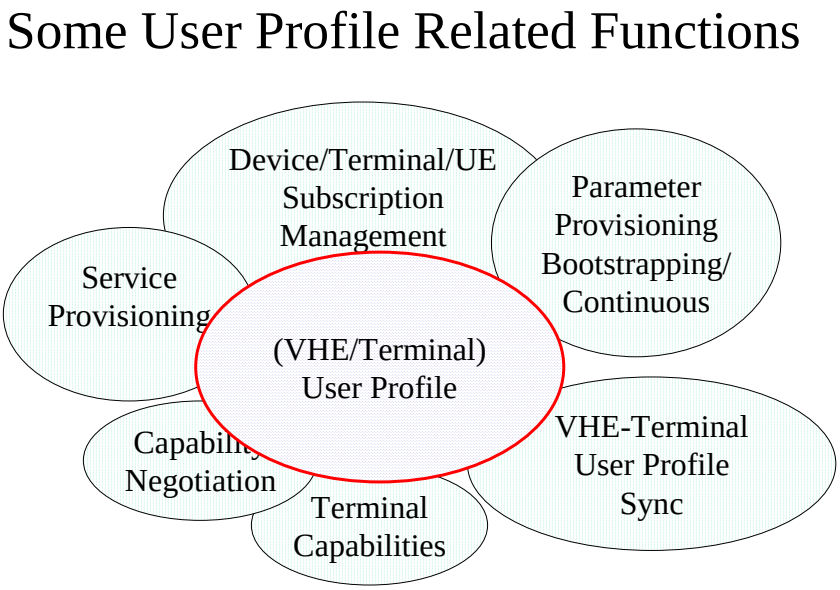


Figure x: Distributed View of the 3GPP Generic User Profile



1. Setting up a Subscription.

- Precondition
  - A person has just purchased a new device, and requires 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 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
  - 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
- 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 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 service provider. User private data is only stored in the network with the user permission.

4. Content Negotiation

[Comment: add Push Stage 1 diagram for 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 ”inter net”

    Deviating capability information
  - Returned content selected or tailored according to User preferences and capability information

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

- Precondition
  - The [OSA] application is registered with the OSA framework
  - The [OSA] 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

6. 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

7. 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

8. 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, 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

9. 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)

Annex <B> (informative): Recommended User Profile content

- General Information
  - Not controlling functions.
  - General User Information (Name, address, age, sex, ID)
  - General Subscriber Information (Name, bill info, users)
- Capability description
  - Describe capacity. Normally not settable.
  - Terminal capability
  - User interface capabilities
  - Communication capabilities
  - Synchronization capabilities
  - MExE capabilities
  - WAP Browser capabilities
- User's preferences
  - User's "wishes". Sent to servers. Used for "content selection".
  - User interface preferences (language, event notifications..)
  - Browser appearance (User's preference for displaying frames)
  - Preferred memory usage
  - IPMM preferences
- Parameters
  - User interface (Ring volume, Vibrating alert, Ring signals, Melodies, Key sound)
  - WAP Parameters (Bookmarks; Gateway: Internet account, Gateway IP address, User ID, Password, Datamode, Security, Show images, Response timer)
  - User security policy (application download, ciphering, positioning)
  - User Security data (Secret keys, user name)
  - Supplementary Services settings
  - IPMM settings (QoS profile, max nob sessions, roaming restrictions)
  - Identifiers/addresses/references (IMSI, IMEI, MSISDN…)

Annex <C> (informative): Change history

Change history										
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New

Version	Date	Comment
0.1.0	Sep 2001	Initial Draft at Sophia Antipolis (UP#3), September 11th-13th 2001
0.1.1	Oct 2001	Cleaned-up version of document for UP#4, based on editorial changes agreed in UP#3
0.3.0	Nov 2001	Includes agreed changes from Stuttgart User Profile ad-hoc , October 10th – 12th 2001
0.4.0	Jan 2002	Structure from S1-020195 adopted
0.5.0	Jan 2002	Agreed changes made after SA1 GUP SWG adhoc, Phoenix 14-18 Jan 2002. Requirements enumerated, structure agreed.
0.6.0	Feb 2002	Changes made to Stage 1 during SA1#15 Saalfelden. Mostly changes to ensure common vocabulary. Section 4.2 added to provide conceptual understanding of GUP. Section 6.1 (Network Requirements expanded)