ETSI TS 102 747 V1.1.1 (2009-12)

Technical Specification

Human Factors (HF);
Personalization and User Profile Management;
Architectural Framework

Reference

DTS/HF-00123

Keywords

profile, user

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Human Factors (HF).

Introduction

The present documents builds on the user profile concept described in EG 202 325 [i.1]. The concept of a user profile usually refers to a set of information, preferences and rules that are used by a device or service to deliver a customized version of capabilities to the user. Traditionally, many devices and services contain profiles specific to that product and unrelated to any other. This requires that, on change of service or device, the user has to re-educate themselves in how to personalize their services or devices and re-enter their information and preferences. This will result in variable success rate and user satisfaction. The user profile concept described in EG 202 325 [i.1] provides an enhanced user experience.

There will be a number of user characteristics and preferences that will apply independently of any particular product (e.g. a user's preferred language or their need for enlarged text). A key objective is that users should not be required to provide this information more times than is necessary.

Users move between situations throughout the day (e.g. at home, driving, working). In each of these situations, users may have different needs for how they would like their ICT resources arranged. At present, an increasing number of products provide the user with ways of tailoring their preferences to these different situations. Users should be able to specify their context dependent needs in ways that require the minimum need to understand the individual products.

In addition, personalization and user profile management holds the promise of improving the uptake of new technologies and allowing greater access to their benefits. The present document provides an architectural framework for supporting personalization and user profile management.

1 Scope

The present document defines an architectural framework supporting the personalization and user profile management concepts described in EG 202 325 [i.1]. The present document addresses issues related to network requirements, functions and procedures. It also covers User Profile security and privacy issues.

Capabilities provided by the architecture are:

- data editing (e.g. creation, templates, update);
- data storage;
- synchronization;
- backup;
- access control respecting user preferences and legal policies;

Profile solutions within the scope of the present document are:

- those provided for the primary benefit of the end-user;
- those which the end-user has rights to manage the profile contents;
- those where the end-user has the right to have a dialogue with the information owning stakeholder.

Intended readers of the present document are user profile providers, operators, service developers, service providers, device manufacturers, standards developers.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI ES 202 746: "Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information".

[2] ITU-T Recommendation M.3050 Supplement 1: "Enhanced Telecom Operations Map (eTOM) - Supplement 1 - Interim view of an interpreter's guide for eTOM and ITIL practitioners".

[3] OMA, Push-to-Talk over Cellular, Architecture.

NOTE: See OMA-AD-PoC-V2_0-20080507-C.

[4] ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

[5] ETSI TS 184 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

[6] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[7] ETSI TS 188 002-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Subscription Management; Part 1: Requirements".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI EG 202 325: "Human Factors (HF); User Profile Management".

[i.2] ETSI TR 132 808: "Telecommunication management; Study of Common Profile Storage (CPS) Framework of User Data for network services and management (3GPP TR 32.808)".

[i.3] ETSI TR 180 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Release 3 definition".

[i.4] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.5] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.6] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.7] UK Home Office; R.V.Clark; "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.

[i.8] ETSI EG 202 067: "Universal Communications Identifier (UCI); System framework".

[i.9] ETSI EG 203 072: "Universal Communications Identifier (UCI); Results of a detailed study into the technical areas for identification harmonization; Recommendations on the UCI for NGN".

[i.10] IETF RFC 4510: "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map".

[i.11] Open Mobile Alliance (OMA): "SyncML Sync Protocol".

NOTE: See http://www.openmobilealliance.org/tech/affiliates/syncml/syncml_sync_protocol_v11_20020215.pdf.

[i.12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.13] United Nations General Assembly resolution 217 A (III) (10 December 1948): "Universal Declaration of Human Rights".

[i.14] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

NOTE: Also available as ISO/IEC 9594-8.

[i.15] ETSI TS 123 240: "Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Generic User Profile (GUP) requirements; Architecture (Stage 2)".

[i.16] Open Mobile Alliance (OMA): "User Agent Profile, Specifications, Version 2.0", OMA-TS-UAProf-V2-0-20060206-A.

[i.17] Open Mobile Alliance (OMA): "Device Profile Evolution V1.0".

NOTE: See http://www.openmobilealliance.org/Technical/release_program/dpe_V1_0.aspx.

[i.18] Open Mobile Alliance (OMA): "Device Management Working Group".

NOTE: See http://www.openmobilealliance.org/Technical/DM.aspx.

[i.19] Open Mobile Alliance (OMA): "Device Management Protocol, Specifications", OMA-TS-DM-Protocol-V1-2-1-20080617-A.

[i.20] Open Mobile Alliance (OMA): XML Document Management V1.1.

NOTE: See http://www.openmobilealliance.org/Technical/release_program/xdm_v1_1.aspx.

[i.21] Open Mobile Alliance (OMA): Presence Simple V1.1.

NOTE: See http://www.openmobilealliance.org/Technical/release_program/presence_simple_v1_1.aspx.

[i.22] ETSI ES 283 030: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service Capability; Protocol Specification [3GPP TS 24.141 V7.0.0, modified and OMA-TS-Presence-SIMPLE-V1-0, modified]".

[i.23] Open Mobile Alliance (OMA): "Instant Messaging and Presence Service V1.3".

NOTE: See http://www.openmobilealliance.org/Technical/release_program/imps_v1_3a.aspx.

[i.24] "OMA-TS-XDM-Core-V1-0-20051103-C" and "OMA-TS-XDM-Shared-V1-0-20051006-C".

[i.25] ETSI TS 183 038: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Simulation Services; Extensible Markup Language (XML) Document Management; Protocol Specification (Endorsement of OMA-TS-XDM-Core-V1-0-20051103-C and OMA-TS-XDM-Shared-V1-0-20051006-C)".

[i.26] Open Mobile Alliance (OMA): "Enabler Release Definition for XML Document Management Candidate Version 2.1", 31 March 2009, OMA-ERELD-XDM-V2-1-20090331-C.

NOTE: See http://www.openmobilealliance.org/Technical/release_program/docs/XDM/V2_1-20090331-C/OMA-ERELD-XDM-V2_1-20090331-C.pdf.

[i.27] IETF RFC 4825: The Extensible Markup Language (XML) Configuration Access protocol (XCAP).

NOTE: See http://www.ietf.org/rfc/rfc4825.txt.

[i.28] "W3C Recommendation: "XQuery 1.0: An XML Query Language", January 23 2007.

NOTE: See http://www.w3.org/TR/xquery/.

[i.29] "W3C Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies", G. Klyne, F. Reynolds, C. Woodrow, H. Ohto.

NOTE See: http://www.w3.org/TR/2007/WD-CCPP-struct-vocab2-20070430/.

[i.30] "W3C Mobile Web Initiative (MWI) Device Description Repository (DDR)".

NOTE: See http://www.w3.org/TR/2007/WD-ddr-core-vocabulary-20071218/#sec-introduction.

[i.31] "W3C Delivery Context Ontology (DCO)".

NOTE: See http://www.w3.org/2007/uwa/editors-drafts/DeliveryContextOntology/2007-11-30/DCOntology.html.

[i.32] ETSI EG 284 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks (NGN)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 325 [i.1] and the following apply:

Concealable, Removable, Available, Valuable, Enjoyable, and Disposable (CRAVED): classification scheme to determine the likelihood that a particular type of item will be the subject of theft [i.7]

context: any information that can be used to characterize the state of entities that are considered relevant to the interaction between a user and an application, network function, service or device

normal profile: user view of information, preferences and rules that are always active in the profile when no specific situation is applicable

object: profile data with attributes, values and operations that the user can refer to when defining their profiles

profile: total set of user related information, preferences, rules and settings which affects the way in which a user experiences terminals, devices and services

NOTE: The use of the word profile in the present document implies user profile unless otherwise stated.

root profile: part of the profile held by the profile provider

situation profile: user view of user related information, preferences and rules which affects the way in which a user experiences devices and services in a specific situation

subscriber: person or organization responsible for concluding contracts for the services subscribed to and for paying for these services

NOTE: See ITU-T Recommendation M.3050.1 [2].

3.2 Abbreviations

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

3GPP AKA	3GPP Authentication and Key Agreement
AA	Attribute Authority
AC	Attribute Certificate
AS	Application Server
ASF	Application Server Function
CA	Certificate Authority
CC/PP	Composite Capability/Preference Profiles
CPS	Common Profile Storage
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
CSCF	Call Session Control Function
CSP	Communications Service Provider
DAC	Discretionary Access Control
DM	Device Management
DPE	Device Profile Evolution
FE	Functional Entity
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GUP	3GPP Generic User Profile
GUPR	3GPP Generic User Profile Data Repository
GUPS	Generic User Profile Server
ICT	Information and Communications Technologies
IMS	IP Multimedia System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
NGN	Next Generation Network
OWL	Ontology Web Language
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PoC	Push to Talk Over Cellular
PSTN	Public Switched Telephone Network
PUA	Personal User Agent
RAF	Repository Access Function
RBAC	Role Based Access Control
RDF	Resource Description Framework
RP	Reference Point
SA	Security Associations
SA	Service Agent
SAML	Security Assertion Markup Language
SIP	Session Initialization Protocol
SOA	Source of Authority
SS	Service Server
SSO	Single Sign On
SuM	Subscription Management
TGS	Ticket Granting Server
TLS	Transport Layer Security
TVRA	Threat Vulnerability and Risk Analysis
UAProf	User Agent Profile
UCI	Universal Communications Identifier
UDF	User Data Function
UE	User Entity
UE	User Equipment
UP	User Profile
UPM	User Profile Management
UPSF	User Profile Server Function

URI	Uniform Resource Identifier
USB	Universal Serial Bus
WAP	Wireless Application Protocol
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XML	eXtensible Markup Language

4 Summary of profile

The role of profiles is to enable all the devices and services used by a user to share the user's preferences and to adapt to the environment in which the device or service is invoked.

NOTE 1: A detailed description of the personalization and user profile concept is to be found in EG 202 325 [i.1].

A user profile is a data object that stores information in the form of profile data items and rules whose value represents preferences related to a particular user for use by a device or service. The definition of the profile data items inside the profile is given in ES 202 746 [1]. The key aim of the architecture is to allow many devices to share a single profile, either in full or in part (referred to as a profile component), and to allow some profile data items of the profile to be set depending on the context in which the device or service is operating.

NOTE 2: In the present document the term profile is synonymous with user profile and is used except where it is essential to distinguish user profile from (for example) service profile.

The management of profiles is carried out using the capabilities of the User Profile Management (UPM) system defined in clause 5.

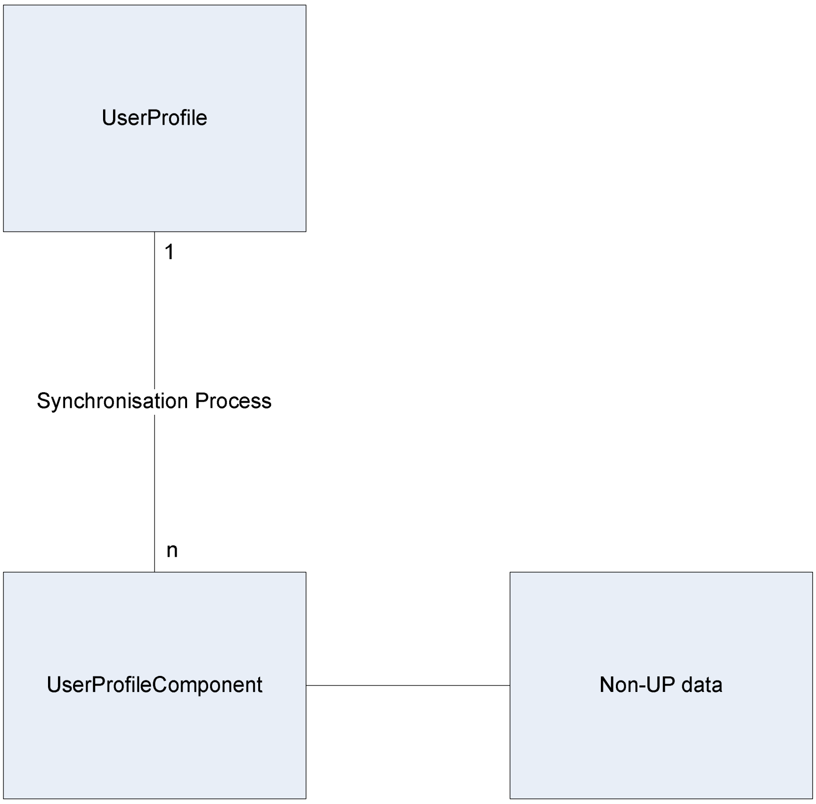


Figure 4.1: Profile components

Whereas in the present document the user profile is considered as if it is a single data entity in practice parts of this profile (user profile components) may be distributed amongst a number of storage locations that include the user's services and devices. The architecture shall support the synchronization process outlined in clause 5. Devices and services shall support the use of profiles (i.e. the use of externally provided configuration data).

It is assumed that in locations where there are profile components in use that there may also be device, service or context specific "Non-UP data" that do not form part of the user profile and thus are excluded from the synchronization process.

The setting of profile data items may be overridden by context data. The profile content when initially invoked is termed the "normal" profile and any modification of the settings of elements by the situation may be referred to as the "situation profile". The term "active" profile is used to refer to the set of profile data items and the settings of those profile data items that are active at the observation point (i.e. at the device or service using the profile).

NOTE 3: If the value assigned to an element is set by the device and/or service context the resultant value may or may not be synchronised with the profile maintained by the profile provider.

The data model, and its coordinating system model, is defined in ES 202 746 [1] and copied below in figure 4.2.

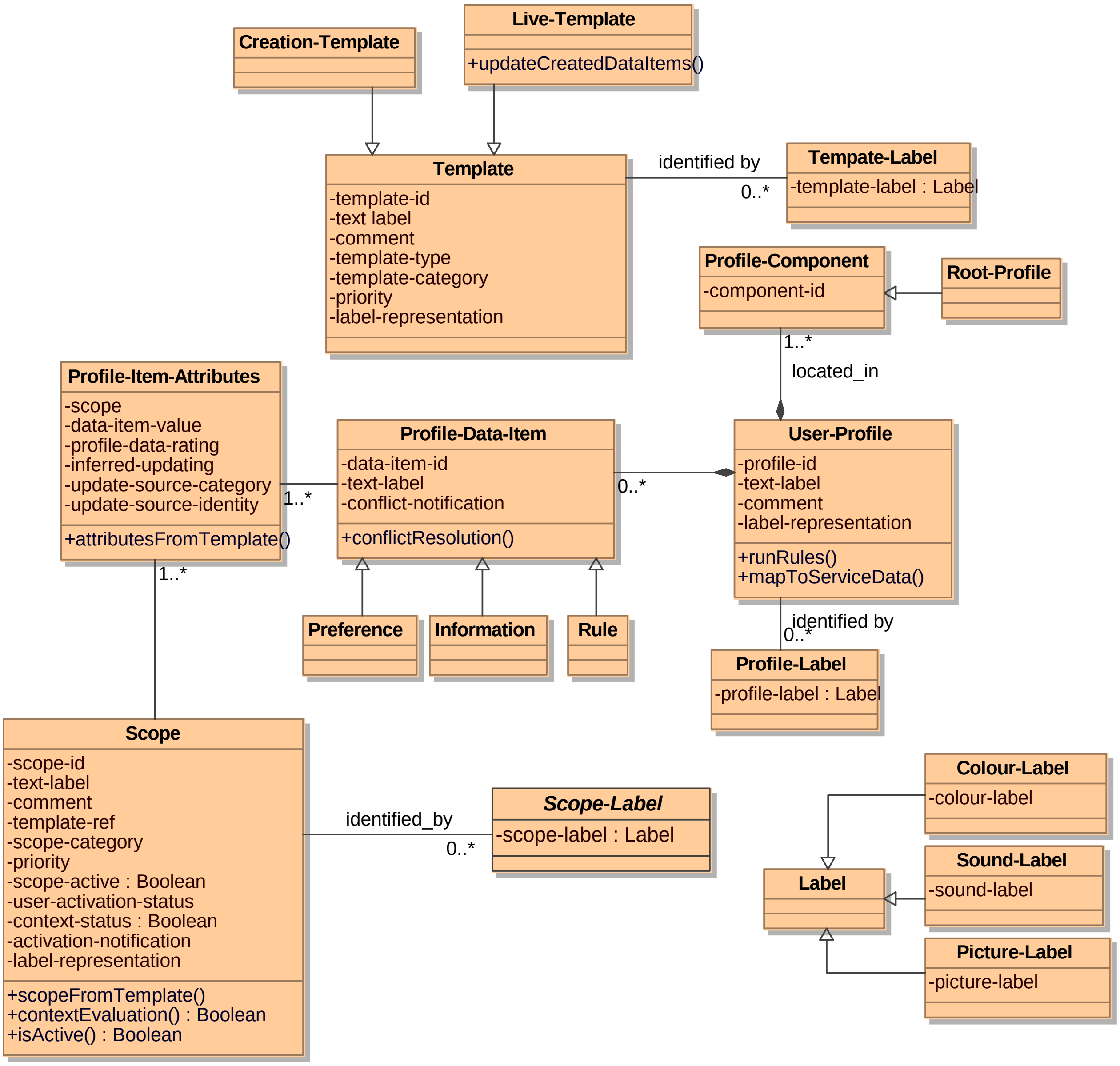


Figure 4.2: UPM system model (from clause 5 in ES 202 746 [1])

As defined in ES 202 746 [1] the central object is the Profile which contains a number of Profile-Data-Items which are defined as one of 3 types:

- preference;
- information;
- rule.

The Profile stores the UPM user's specific personalization requirements at any time.

In addition to profile data items as defined and listed in ES 202 746 [1], it is expected that there will be a need for future additional standardized information and preferences, for which new versions of [1] will be developed. Furthermore, it is possible for service developers and device manufactures to include proprietary profile data items in the profile which shall be identifiable as proprietary (e.g. specify the company and/or product identifier for which the proprietary information and preferences are intended for). Proprietary profile extensions are outside the scope of the present document.

5 User profile management architecture requirements

5.1 Profile roles

As defined in EG 202 325 [i.1] the user may play two roles:

- Profile user:
    - role played by end users when using a profile.
- Profile administrator:
    - role played by end users when defining or modifying a profile.

The same end user can play both the user role and the administrator role.

5.2 Profile identification

The profile seen by the user at the device or service using the profile should be readily identifiable by the user and may therefore be identified by name, icon (or other visual mnemonic), or other user interpretable indication (as defined in ES 202 746 [1]). All instances of the profile shall share this identity but the presentation of the identity shall be defined by the users' device or service specific preferences.

The profile user should be given the option by the profile administrator of using predefined instances of a profile in the form of templates. These templates may contain pre-defined rules for reacting to the context (e.g. predefined rules for setting profile data items to particular values based on context. The suite of rules and settings should be presented to the user in a readily identifiable way and may be considered by the user as profile instances (such as the situation profiles home profile and meeting profile).

A profile administrator should, in addition, be provided with tools to edit the content of a profile.

5.3 The UPM architecture model

The UPM architecture is derived from the use cases and their interaction illustrated in figure 5.1, and the class model that may be developed in figure 5.2.

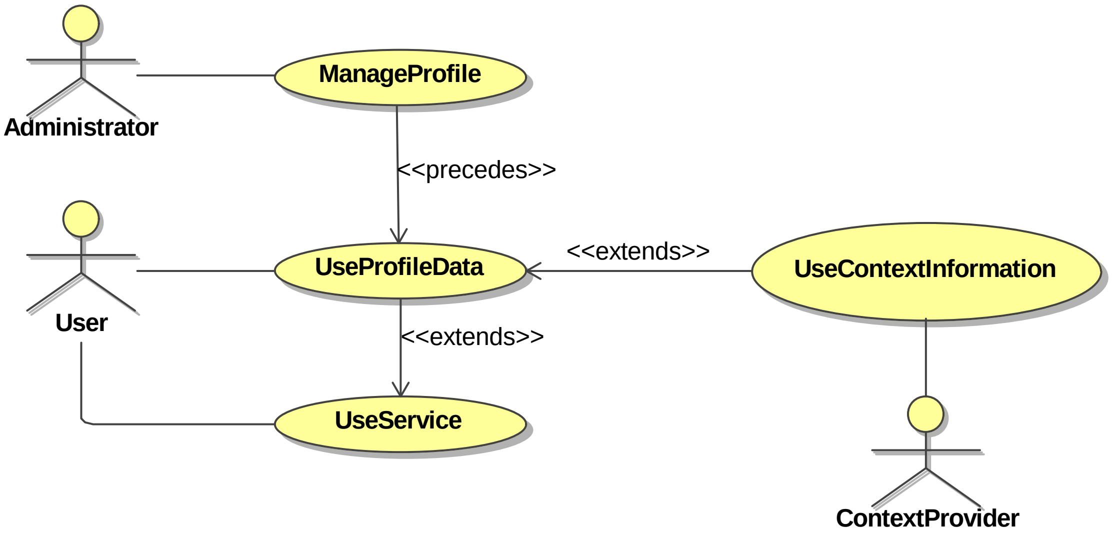


Figure 5.1: Simplified model of UP/UPM

The "UseService" use case represents the use of all the services available to a user (e.g. communications services, information services, entertainment services). Included in this use case is the use of devices that enable usage of the services. The scope of this use case is all service usage that does not require the existence of a UPM system.

The "ManageProfile" use case relates to the creation and subsequent management of a user's profile.

The "UseProfileData" use case relates to the modification and use of profile data. The goal of the "UseProfileData" use case is to adapt the profile data to ensure that it is compatible with the user's requirements according to the current context and the user's stated preferences.

The "UseProfileData" use case extends the "UseService" use case by adapting service behaviour according to the profile data in order to deliver the user's preferred service usage options. The "UseProfileData" use case thus enables the automation of aspects of service usage that otherwise require explicit user input in the "UseService" use case.

The "UseContextInformation" use case processes context information provided by the ContextProvider actor. The processed context information is used within the "UseProfileData" use case to update the profile data to take account of the current situation that the context data represents.

The "UseContextInformation" use case extends the behaviour of the "UseProfileData" use case by offering it the processed context information. The "UseContextInformation" use case thus enables the automation of context dependent aspects of service usage that could otherwise only be controlled by explicit user input in the "UseProfileData" use case.

The ContextProvider may be any entity or application that provides context information of relevance to the operation of the user's profile. Examples of ContextProvider include presence services, sensors, sensor networks, applications that generate status information (e.g. agendas and task list applications), or the user directly entering information about their current context.

The Universal Communications Identifier (UCI) and its system is defined in EG 202 067 [i.8] and has similarities to the UP/UPM concepts. UCI describes the user management of both inbound and outbound communications and the presentation of the user identity across the communications network. UP/UPM shares the UCI characteristic of user management and extends it to the setting of preferences for the way in which a service or device is presented to the user. The mapping is explained in clause A.1.5 on Universal Communications Identifier.

A class based model of UP/UPM that is derived from the use case model given in figures 5.1 and 5.2.

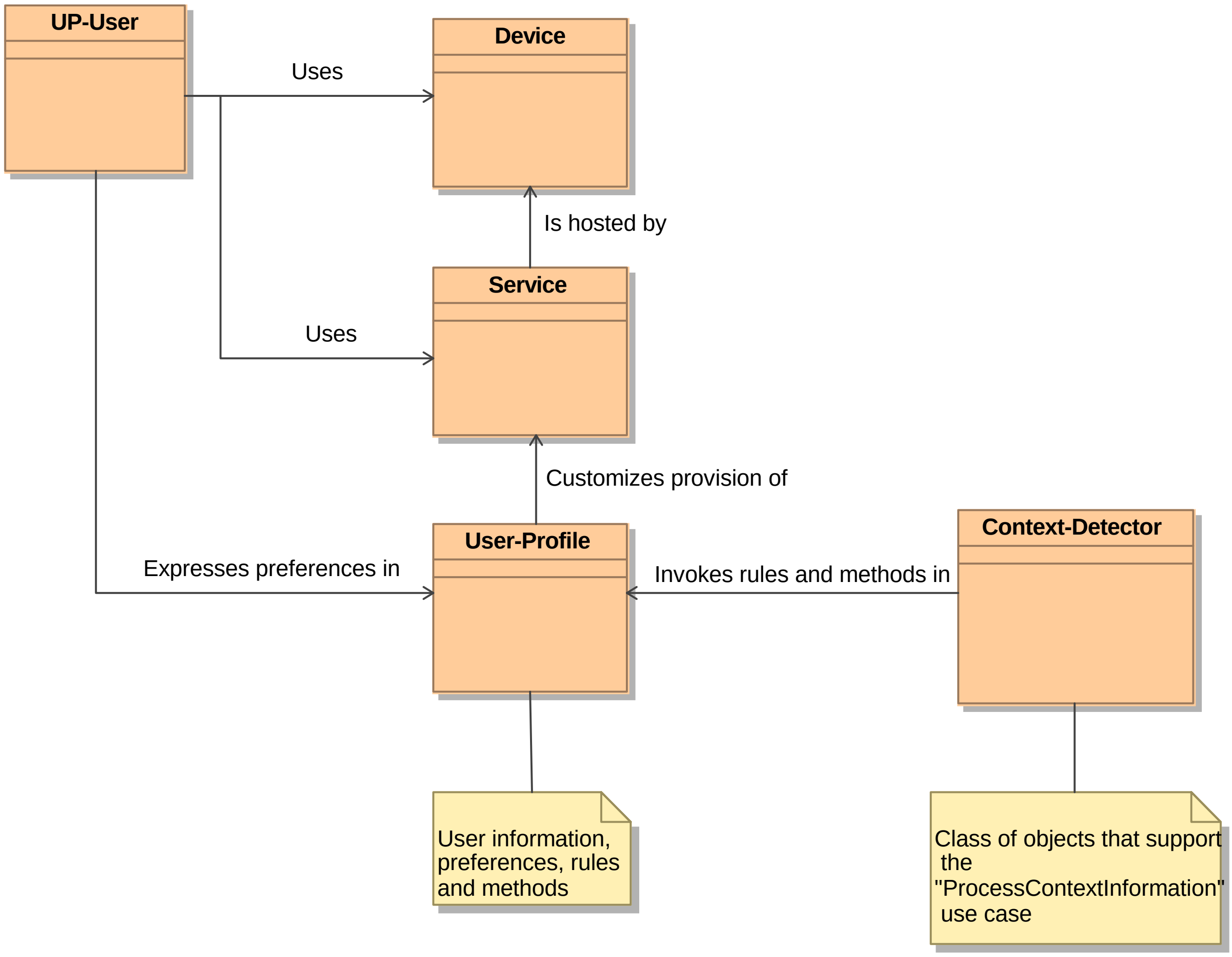

UP-User
Device
Uses
Is hosted by
Service
Uses
Customizes provision of
User-Profile
Context-Detector
Expresses preferences in
Invokes rules and methods in
User information, preferences, rules and methods
Class of objects that support the "ProcessContextInformation" use case

Figure 5.2: Class interaction model for UP/UPM based on use case model

The services and devices that are customised by application of the profile are those of the host system using UP/UPM, e.g. the NGN.

Further details on mapping with networks and services are provided in clause A.1.

5.4 Procedures

NOTE: Whilst many of the user initiated interactions outlined in this clause require an intuitive user interface, details of the user interface are not defined in the present document.

5.4.1 Introduction

UPM shall support the following procedures described in detail in the present document:

- Profile synchronization.
- Profile creation/update.
- Modification of profile data according to context.
- Profile deletion.

The procedures listed above are considered with respect to the use case model provided in figure 5.1.

The Administrator should invoke the use case "ManageProfile" in order to create and modify data in the user's profile.

The "UseProfileData" use case can be directly invoked by the user through one or more applications that require or are able to use externally sourced configuration and personalization data.

NOTE: It is a pre-requisite that the application which will use the profile is UP/UPM aware (or compatible) in order for UP/UPM to be enabled.

The "UseContextInformation" use case is invoked when the Context Provider actor provides new or updated context information. The "context watcher" is an active application that performs the "UseContextInformation" use case. It gathers, integrates and presents context related data made available from the various context sources (e.g. presence services, sensors, sensor networks, applications that generate status information such as agendas and task list applications). The user may also directly enter information about their current context in the "UseContextInformation" use case.

In a TISPAN NGN context, the Presence Service delivers most of the functionality of a "context watcher" application.

5.4.2 Profile synchronization

Data values in the profile shall be updated by means of the device or service native functionality. Where values in the profile are to be exported for common application, the methods in this clause shall apply.

NOTE: The term service includes those applications used for direct management of the profile as well as those used for user services (e.g. address book manager).

If the content of a profile component has been changed in the device or service, then the user may be given the option to update the root profile (held by the profile provider) with these changes such that they then become available to other profile components. The synchronization scenarios described in table 5.1 shall be supported by the synchronization protocol where the profile component in use at the device or service is considered the database client, and the root profile held by the profile provider is considered as the database server.

Table 5.1: Synchronization scenarios to be supported in UP/UPM

Sync Scenario	Description
Two-way sync	The client and the server exchange information about modified data in both the profile component (at the client) and the root profile (at the server). The client sends the modifications first.
One-way sync from client only	The client sends its modifications made in the profile component to the root profile to the server but the server does not send its modifications back to the client.
Refresh sync from client only	The client sends all the profile component data to the server. The server is expected to replace all corresponding data in the root profile with the data sent by the client.
One-way sync from server only	The client receives all the root profile modifications from the server but the client does not send its modifications to the server.
Refresh sync from server only	A sync type in which the server sends all its data from a database to the client. The client is expected to replace all data in the target database with the data sent by the server.

A model of the basic synchronization protocol in the form of a message sequence chart is given in figure 5.3.

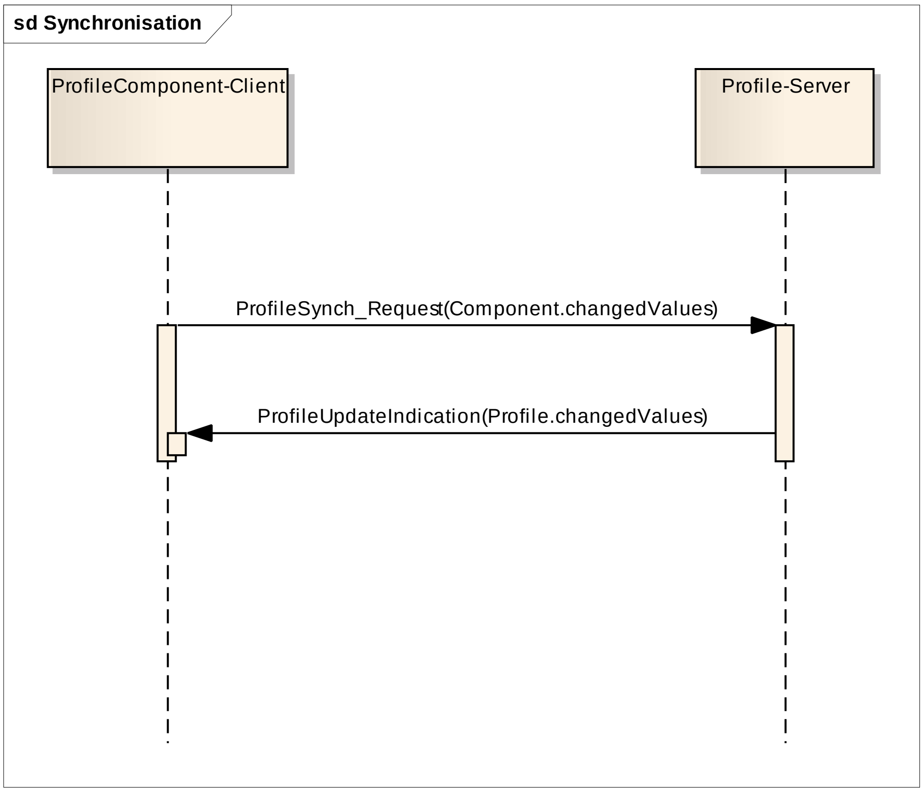

sd Synchronisation
ProfileComponent-Client
Profile-Server
ProfileSynch_Request(Component.changedValues)
ProfileUpdateIndication(Profile.changedValues)

Figure 5.3: Synchronization sequence

5.4.2.1 Synchronization conflict resolution/avoidance

Conflicts may occur in the setting of a profile data item value in the root profile storage when two (or more) profile components attempt to synchronize that profile data item where each component holds a different value for the element. To avoid this any update transaction shall lock out any other update transactions.

NOTE: This means that a single user trying to update the root profile from two devices at nearly the same time may see a delay on one device receiving confirmation that the update has been completed, or may receive a warning that the root profile cannot be updated as it is locked by the other user and device.

5.4.2.2 Protocol candidates for profile component synchronization

The present document does not define the detail protocol to implement the synchronization of profile components to the root profile. This clause illustrates the availability of protocols that may fulfil the requirements previously indicated.

When treating UP and UPM as a means of harmonizing database content there are a number of candidate protocols for implementing the synchronization of database components. The two primary candidates are Lightweight Directory Access Protocol (LDAP) defined in RFC 4510 [i.10], and Open Mobile Alliance Data Synchronization and Device Management suite (formerly known as SyncML) defined in OMA SyncML Sync Protocol [i.11].

In an NGN environment the native synchronization protocol for the NGN shall be used.

5.4.3 Profile creation/update/deletion

5.4.3.1 Profile creation

The suite of procedures for creation/update/deletion of the profile includes the following cases:

- Creation of a root profile.
- Association of a root profile to service or device (creation of a profile component).

NOTE: A template or an existing profile can be used as the starting point for creation of a new profile or situation profiles.

Identification of the root profile storage location shall be by a Uniform Resource Identifier (URI) indicating both the protocol and location used to access the root profile storage location.

A profile storage broker may offer predefined profiles to be used as a template for the creation of new profiles.

5.4.4 Update of profile data according to context

The most important task of the UPM system is to ensure that the values of the attributes of Profile-Data-Items meet the user's preferences for the current context. This shall be achieved by using the following simple algorithm (see the method named conflictResolution in ES 202 746 [1]) that sets the values of the attributes of a Profile-Data-Item:

- Step 1: all active Scope objects that are associated with the Profile-Data-Item shall be identified. The number found = n.
- Step 2: then the following procedure shall be followed:
    - If n = 0 then take no action.
    - If n = 1 then the attributes of the Profile-Data-Item are those in the Profile-Item-Attributes object associated with the active Scope object.
    - If n > 1 then the priority attribute of the Scope objects are examined and if the priority attribute of one Scope object is greater than that of the other Scope objects:
        - then the attributes of the Profile-Data-Item are those in the Profile-Item-Attributes object associated with the active Scope object with the highest priority;
        - else, a Special Resolution Policy is implemented to resolve what values should be used for the attributes of the Profile-Data-Item.

All UPM systems shall have a Special Resolution Policy. The precise way in which the results of a Special Resolution Policy are calculated is outside the scope of the present document. However it may frequently be decided to request the profile user to propose or confirm all or part of the solution.

The use of well designed templates for creating profiles can be a very effective way of minimising the situation where the Special Resolution Policy needs to be implemented. It is also advisable that profile providers should assist users who wish to modify their profiles by helping them to assign priorities to avoid potential conflicts.

Annex E provides further information on avoiding conflicts by using templates and conflict resolution/avoidance methods that may be used as part of a Special Resolution Policy.

5.4.5 Profile deletion

A user may delete a component or an entire profile from the device or service. Deletion of a root profile where components are in use shall be prevented. When deleting a live template, the profiles created based on it will still remain, but will have to be updated individually instead of being updated through the live template.

6 UP/UPM security

6.1 UP/UPM and impact on privacy

The services and devices that together form the UP/UPM (sub) system should ensure consistency with Article 12 of Universal Declaration of Human Rights [i.13] which declares that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" and thus the UP/UPM system should assure users of the following:

- The privacy of any user should not be compromised by any action of the UP/UPM system.
- The correspondence of a communications system user should not be compromised by any action of the communications system including the UP/UPM subsystem.

It has to be noted however that most personal data transferred over networks, or between users, is in the public domain. Thus a person's name, address, telephone numbers, bank numbers (account numbers and bank codes, credit card numbers, banking offices), email addresses, transport methods, social security details, date of birth, place of birth, details of family and friends, are in the public domain. What is clear is that in a non-networked world the exposure of such public data and the means to exploit them are relatively low and can be controlled. In a networked world the exposure of data is less controlled and hostile agents may be less obviously present.

A further model that may illustrate the concerns related to protection of identity and of privacy is in the link of behaviour and the person. As a person exhibits certain behaviours so those behaviours may act to identify the person. In a communications environment those behaviours may be visible from points on the network (for the present document the network is the NGN) and thus the network may be able to identify a person from examination only of behaviour.

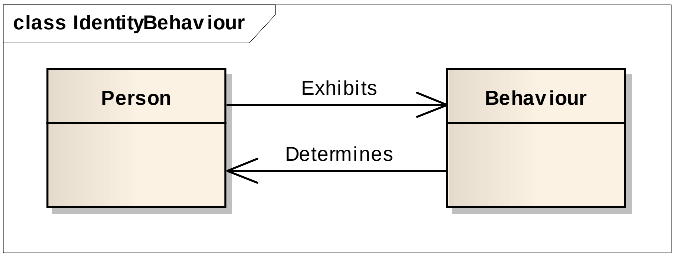


Figure 6.1: Link between person and behaviour

The content of the profile may have data that uniquely identifies a person, or by examination only of the behaviour associated with the use of data in a profile may uniquely identify a person. It is important therefore to ensure that the risk of identification of a person through malicious access to the profile or the behaviour inherent in the use of the profile is minimised.

6.2 Key goal for UP/UPM security

For UP/UPM the intent is to ensure a set of applications can use the data in a profile, and have trust in that data, without having to establish a security relationship in advance with the user or with the data.

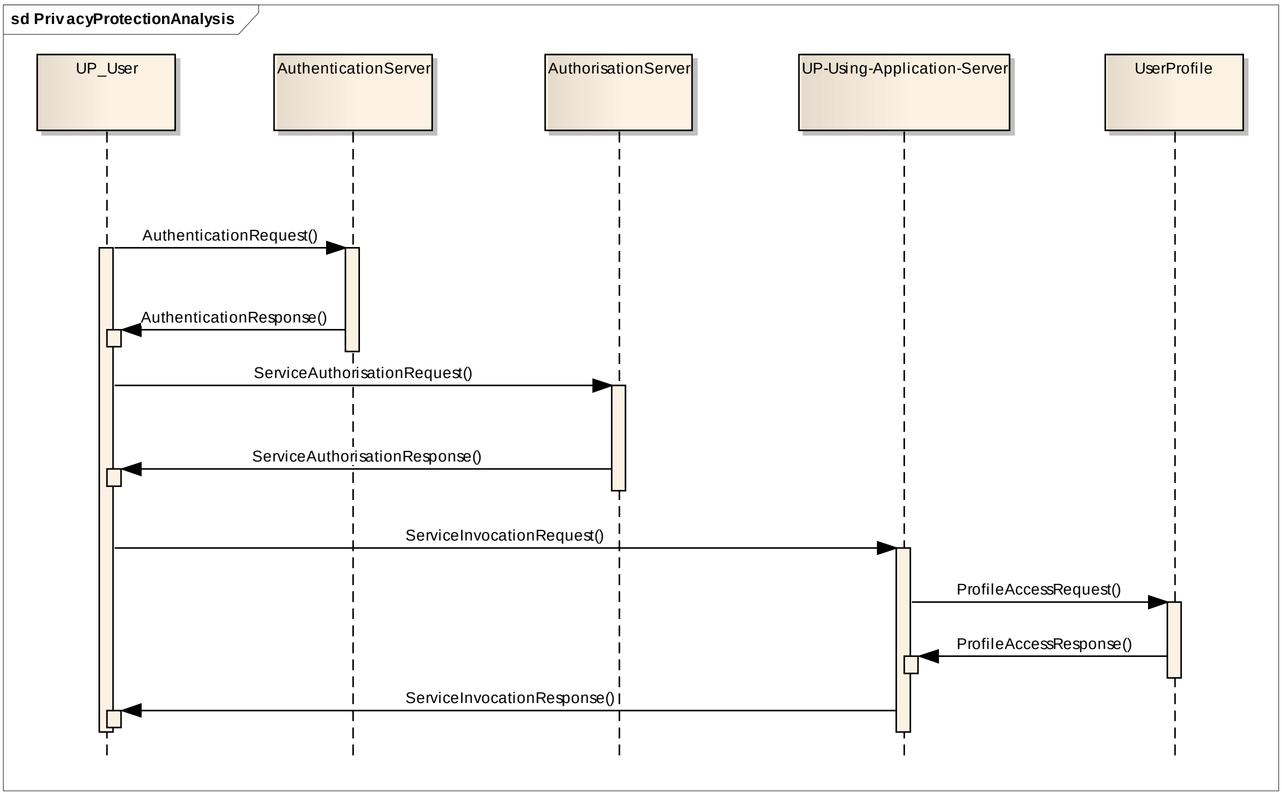
NOTE: There will be a residual risk associated with UP/UPM and a strong likelihood of leakage of private data when using personal devices due to the nature of the devices. In particular as many of the UP/UPM enabled devices are likely to be attractive to criminals (i.e. they meet the key characteristics of a CRAVED [i.7] entity) there is an increased opportunity for criminals to break any user provisioned security features.

For the purposes of analysis the assumptions listed in table 6.1 are made with respect to profiles and profile components.

Table 6.1: Assumptions related to UP/UPM components

	Assumption
Assumption#1	Profile components may extend the data held in the profile
Assumption#2	Many profile components may contain the same profile data items from the root profile
Assumption#3	Many profile components may exist concurrently (i.e. many devices requiring a profile may be active at the same time)
Assumption#4	Not all profile data items are mutable in the component
Assumption#5	Profile extensions (not subject to synchronization) may exist alongside any component
Assumption#6	A profile is associated to a device and not part of a device (a UP enabled device is assumed here to include a software application)
Assumption#7	Multiple software applications may exist in the same physical device

The dynamic behaviour for securing use of the profile is summarised in figure 6.2.


sd PrivacyProtectionAnalysis
UP_User
AuthenticationServer
AuthorisationServer
UP-Using-Application-Server
UserProfile
AuthenticationRequest()
AuthenticationResponse()
ServiceAuthorisationRequest()
ServiceAuthorisationResponse()
ServiceInvocationRequest()
ProfileAccessRequest()
ProfileAccessResponse()
ServiceInvocationResponse()

NOTE 1: The interaction of the user with both the Authentication Server and the Authorisation Server extends the use case "Registration".

NOTE 2: The interaction of the user with the Authorisation Server extends the use case "UseProfileData".

Figure 6.2: Dynamic overview of UP for security analysis

The dynamic overview maintains separation of authentication and authorisation (as a means to enable access control). Authorisation is not a property of the profile itself but is provided by the UP/UPM system and therefore is not visible as an element in the profile.

6.3 Risk analysis - assumptions and objectives

For the purposes of analysis the assumptions listed in table 6.2 are made with respect to UP/UPM.

Table 6.2: General assumptions related to UP and UPM

	Assumption
Assumption#1	A user profile is shared between devices
Assumption#2	Devices may use the same profile concurrently
Assumption#3	Devices may be provided with sensors to modify the contents of the profile (context driven profiles)
Assumption#4	The structure of a profile is not considered personal but the content is
Assumption#5	The master profile is not always available to the device
Assumption#6	A profile can be marked as "master" or "component"
Assumption#7	The values of profile data items in a profile may indicate the current behaviour of the profile user
Assumption#8	Values of profile data defined as enumerations cannot be extended by the UP user
Assumption#9	Values of profile data defined as enumerations cannot be extended by the UP administrator
Assumption#10	The same person can act in both user and administrator roles
Assumption#11	For NGNs the UP user is a special case of the NGN user

The primary security concerns for UP/UPM are related to the protection of privacy of user data. The right to privacy is enshrined in a number of regulations in Europe and any deployment of UP/UPM and its principles shall be expected to comply to those regulations. The regulation of particular concern is Directive 95/46/EC [i.12] on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and results in the set of security objectives given in table 6.3.

Table 6.3: Security objectives related to UP and UPM

Confidentiality	
Co1	Information sent to or from an authorized UP user should not be revealed to any party not authorized to receive the information.
Co2	Information held within the UP should be protected from unauthorized access.
Co3	Details relating to the identity and service capabilities of an UP user should not be revealed to any unauthorized 3rd party
Co4	Management Information sent to or from an UP should be protected from unauthorized access
Co5	Management Information held within an UP should be protected from unauthorized access
Co6	Personal data pertaining to a user should be collected by the hosting network using legitimate means only
Co7	No change in the ownership, responsibility, content or collection of personal data pertaining to a the user profile should occur without that user's consent or knowledge
Co8	No action of the hosting network should make a user liable to be the target of identity crime
Integrity	
In1	Information held within an UP should be protected from unauthorized modification and deletion
In2	Information sent to or from a registered UP user should be protected against unauthorized or malicious modification or manipulation during transmission
In3	Management Information held within a UP should be protected from unauthorized modification and deletion
In4	Management Information sent to or from an UP should be protected against unauthorized or malicious modification or manipulation during transmission
In5	The content of a user profile should not be compromised by any action of the hosting network
Availability	
Av1	The UP should only be available to services when authorized by the UP owner
Av2	Access to and the operation of UP services by authorized users should not be prevented by malicious activity within the hosting environment
Av3	Access to the content of user profiles should only be granted to users with appropriate authorization
Accountability	
Ac1	It should be possible to audit all changes to security parameters and applications (updates, additions and deletions)
Ac1	An audit trail of all transactions having an impact on personal data pertaining to users should be maintained within the hosting network
Authenticity	
Au1	It should not be possible for an unauthorized user to pose as a legitimate and authorised user when interacting with the UP
Au2	It should not be possible for an UP to receive and process management and configuration information from an unauthorized user

Privacy	
Pr1	Information able to identify a user shall be protected from unauthorised disclosure
Pr2	The privacy of an user should not be compromised by any action of the UP/UPM system
Pr3	The correspondence of a communications system user should not be compromised by any action of the communications system including the UP/UPM subsystem
NOTE: The hosting network is assumed to be the NGN as specified in TISPAN and in particular the core capabilities of TISPAN NGN-R3 defined in TR 180 003 [i.3] are assumed.	

A consequence of the "authority" requirement is the association of identity and the key capabilities of identification and verification of identity (authentication).

6.4 Risk analysis - functional capabilities

NOTE: The functional capabilities are derived using the guidelines given in TR 187 011 [i.5] and form a part of the ETSI TVRA approach to risk based security provisions as defined in TS 102 165-1 [i.4].

6.4.1 Threats and threat agents in UP/UPM

The primary threats and attack forms to be considered in UP/UPM are:

- Masquerade as UP/UPM user or as UP/UPM service provider.
- Interception of UP/UPM data in transit or from storage.
- Manipulation or UP/UPM data in transit or in storage.

In addition the system should be able to prevent replay attacks (in this case to allow a session or message to be replayed and thus allow an attacker to use intercepted credentials). The system however should not require accurate clock synchronization to prevent replay but should rely upon validation of nonces at the receiving system which is consistent with a cryptographic approach to replay protection.

The UP/UPM system is most vulnerable to attack during synchronization as data is transferred and thus open to interception and manipulation. In addition as both the profile components and the root profile belong to a single user and that user may be active in many locations (devices and services using the profile) concurrently, there is significant risk of interception of the user behaviour and identity revealing data that without adequate protection may lead to masquerade.

6.4.2 Identification

Management and user actions in UPM that lead to a change in the profile should be fully accountable and therefore the invoking entity should be identified and should also be authenticated (to counter masquerade). Each invocation of a UPM and/or UP capability should follow the following simple guidelines:

- The <<*UPM/UP invoking user*>> is not allowed to <<*invoke the UPM/UP capability*>> prior to successful identification (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for Identification and Authentication, User Identification before any action (FIA_UID.2)).
- The <<*UPM/UP invoking user*>> is not allowed to <<*invoke the UPM/UP capability*>> prior to successful authentication (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for Identification and Authentication, User Authentication before any action (FIA_UAU.2)).

NOTE 1: Identification may be achieved by a number of schemes.

NOTE 2: Authentication may be achieved by a number of schemes.

NOTE 3: In some cases formal identification and authentication of the invoking party will not be possible, in such cases the invoker should be considered as anonymous and the capabilities offered to anonymous users should be extremely restricted, i.e. should not be able to create or delete permanent (long-life) data.

From an analysis of the UP/UPM system the most significant point of exposure to attack is in the synchronization system.

6.4.3 Privacy

Privacy is inherently complex and there are a number of core functional aspects that have to be addressed. These are summarized in the bullet points that follow:

- **Anonymity:** ensures that a user may use a resource or service without disclosing the user's identity. The requirements for Anonymity provide protection of the user identity.
- **Pseudonymity:** ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.
- **Unlinkability:** ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- **Unobservability:** ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

For the purposes of UPM where the primary actors in the privacy domain are the user's device or service, and the storage manager for the root profile, the key element of privacy that shall be provided by the system is Unlinkability. Unlinkability shall be tied to the provision of Pseudonymity (ensuring observation of a real user name cannot be made).

Each invocation of a UPM and/or UP capability should follow the following simple guidelines:

- The UPM/UP system shall ensure that any third party is unable to determine whether any visible UP/UPM transactions were caused by the same UP user (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for Privacy, Unlinkability (FPR_UNL.1)).
- The UPM/UP system shall ensure that any third party is unable to determine the real user name bound to the UP (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for Privacy, Pseudonymity (FPR_PSE.1.1)).

6.4.4 Integrity (data)

Where data is transferred between any pair of collaborating entities in the context of UPM the integrity of the transferred data should be assured. If the received data is required by an invoked service capability that service capability should be terminated if there is any doubt in the integrity of the received data. Failures in data integrity come in a number of forms: Modification (say changing a bank transaction from 100 € to 10 €); Deletion (say deleting a bank transaction); Insertion (say adding a bank transaction); and Replay (retransmitting a request to force the recipient to redo something).

The UP/UPM integrity protection considers two distinct areas:

- integrity of data across the synchronization process; and
- integrity of data in centralised data stores.

In reviewing the integrity risks the primary risk is seen in the transfer process at synchronization and the requirements listed below counter this risk. Protection against modification, insertion and deletion is mandated whilst protection against replay is strongly recommended.

- The UP/UPM system shall enforce the synchronization process to transmit user data in a manner protected from modification errors (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.1)).
- The UP/UPM system shall enforce the synchronization process to transmit user data in a manner protected from deletion errors (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.1)).
- The UP/UPM system shall enforce the synchronization process to transmit user data in a manner protected from insertion errors (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.1)).

- The UP/UPM system should enforce the synchronization process to transmit user data in a manner protected from replay errors (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.1)).
- The UP/UPM synchronization system shall be able to determine on receipt of user data, whether modification has occurred (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.2)).
- The UP/UPM synchronization system shall be able to determine on receipt of user data, whether deletion has occurred (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.2)).
- The UP/UPM synchronization system shall be able to determine on receipt of user data, whether insertion has occurred (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.2)).
- The UP/UPM synchronization system should be able to determine on receipt of user data, whether replay has occurred (wording derived from ISO/IEC 15408-2 [i.6] functional capabilities for user data protection, data exchange integrity (FDP_UIT.1.2)).

NOTE: Detection of integrity errors may be achieved by a number of schemes.

6.5 Detailed security requirements

The detail security requirements are provided in the present document at an abstract level to allow them to be mapped to provisions in existing mechanisms that may be deployed in the target environment for UP/UPM.

As identified in annex D the core of security is in the provision of Security Associations (SAs) and for the purposes of communications security in UP/UPM the primary protocol to secure is the synchronization protocol outlined in clauses 5.3 and 5.4 as that protocol exchanges parts of the profile across a supporting network.

6.5.1 Identification SA

Accurate identification of the UP user, the UP enabled devices and services, and the UP storage area is essential as a pre-condition for authentication and may be an essential pre-condition for authorization.

In the general case the UP-user is a person and shall adopt the naming scheme of the system that hosts the UP/UPM enabled devices and services. Where the host system is the NGN the UP-User shall be identified as an NGN-user as identified in TS 184 002 [5] (see figure 6.3).

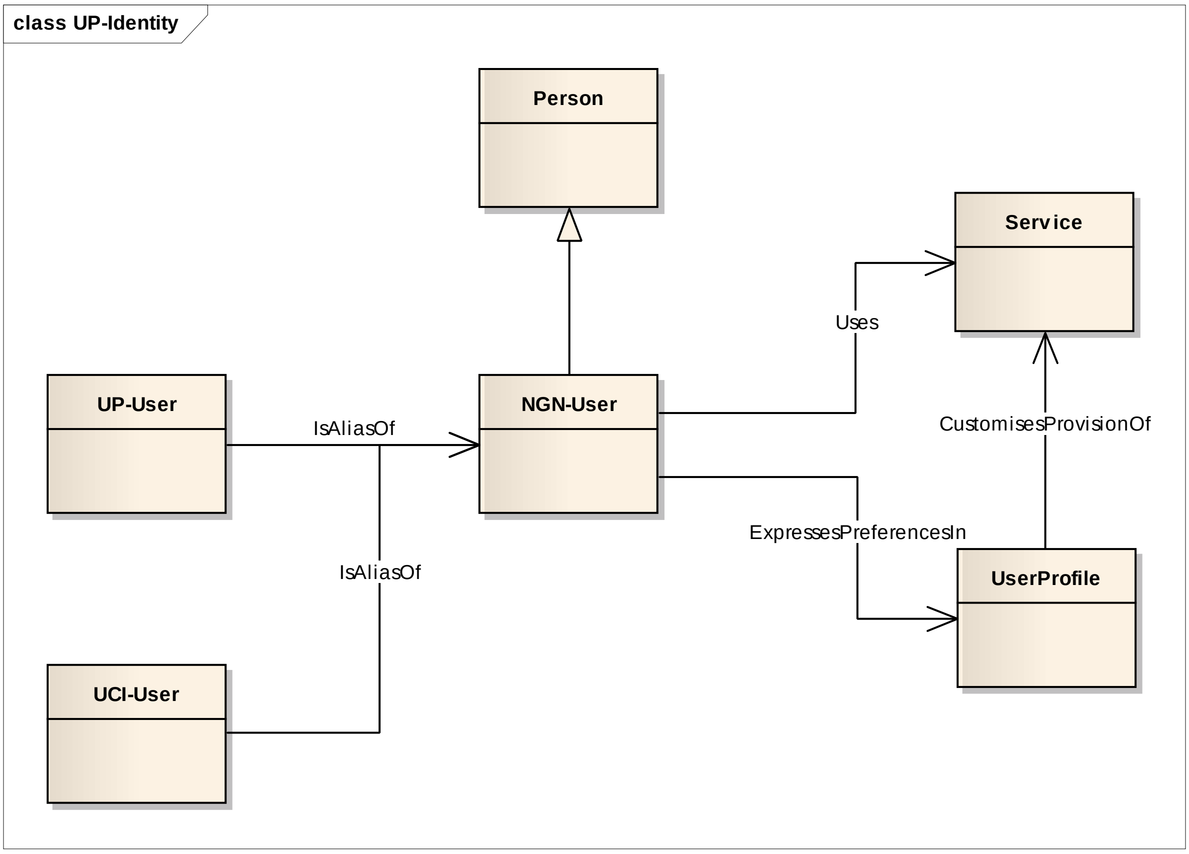


Figure 6.3: Identification of UP-user as alias of NGN-user

6.5.2 Authentication SA

Where the host system is the NGN and where the UP-User is identified as an NGN-user as identified in TS 184 002 [5] the authentication schemes identified for the NGN shall apply.

6.5.3 Authorisation SA

In order to ensure that only authorized parties can access and update the profile there shall be an authorization SA between the parties involved in the synchronization protocol, i.e. the profile service provider hosting the root profile and the device or service holding the active profile.

The form of Authorisation SA shall be a Privilege Management Infrastructure (PMI). A short summary of approaches to PMIs is given in annex F.

6.5.4 Confidentiality SA

In order to preserve privacy of communication and to protect from exploit of intercepted data there shall be a confidentiality SA between the parties involved in the synchronization protocol, i.e. the profile service provider hosting the root profile and the device or service holding the active profile.

6.5.5 Integrity SA

The UP/UPM system shall provide integrity services (generation of proof of integrity and validation of the proof) across all connections and for the data storage areas.

Annex A (normative): Mapping to services and networks

A.1 Introduction

The user profile system defines a functional architectural framework supporting the personalization and user profile management concepts described in EG 202 325 [i.1]. In order to make this profile system operable with a range of services networks in a seamless way, it is necessary to be able to include it into the standardized network architecture. The following clauses describe the Mapping of user profile roles with TISPAN roles and identify standard Functional Entities (FE) and Reference Points (RP) which could be possible candidates for implementing the UPM architecture.

A.1.1 Mapping of user profile roles with TISPAN roles

A.1.1.1 Introduction

This clause maps user profile roles with roles defined in TISPAN [7], with the purpose to specify further mappings with the TISPAN architecture.

NOTE: While the shorter forms "profile user" and "profile administrator" are used in the present document, the longer forms "user profile user" and "user profile administrator" are used in this clause in order to make it clear that in the TISPAN context, those roles address the use/management of user profiles as described in the present document. It does not address any other profiles used in the TISPAN context.

A.1.1.2 Principles

The following principles apply:

- The user profile administrator shall be able to manage any information, preferences and rules a TISPAN service user can manage.
- The ability to use and manage services by means of the user profile system shall not permit TISPAN users and subscribers to have greater rights than they would have without the use of the user profile system.
- Thus, if the entity managing information, preferences and rules related to TISPAN services is required to be a service subscriber, then the user profile administrators shall be able to perform that management only if they are also service subscribers.

A user profile administrator shall not be able to use the user profile system to perform functions assigned to a service subscriber (rather than to a user) unless the user profile administrator is also the subscriber to that service.

EXAMPLE: A parent may act as a profile administrator for a child (maybe an older child), but the parent will not be permitted, without having been granted explicit rights, to perform profile administrative functions that relate to a service for which the child is also the subscriber. For parts of the profile that relate to this service, the child would have full administrative rights.

According to what is described above, there are two different cases (table A.1). In the first case, the user profile administrator and the user profile user are both users (TISPAN role), in the second case the user profile administrator is a subscriber (TISPAN role).

NOTE 1: Wherever TISPAN role is used it should be understood as the role defined by the ETSI TC TISPAN for NGN.

Table A.1: User profile roles

user profile role	**case 1**(TISPAN role)	**case 2** (TISPAN role)
user profile administrator	user	subscriber
user profile user	user	user

NOTE 2: Whenever user profile administrators are also subscribers, they are called "user profile administrator who is a subscriber".

To further clarify; the user profile administrator in case 1 above would be restricted to modifying those parts of their profile that relate to things that they would be allowed to do as an ordinary service user. For example, they would be allowed to update that part of the profile that relates to the chosen destination for call forwarding supplementary services.

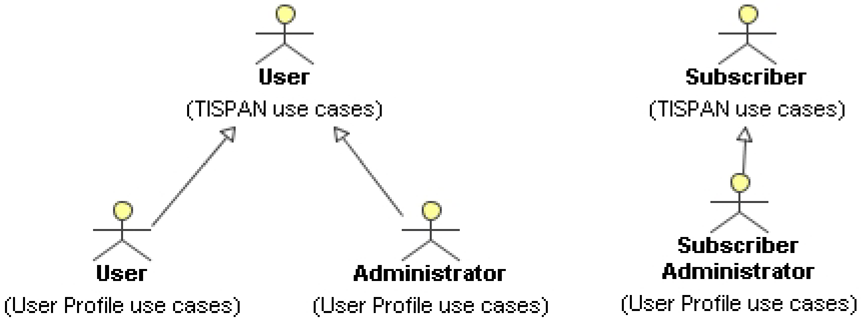


Figure A.1: User Profile roles and relationships mapped to roles used in TISPAN

A.1.1.3 Involved use cases

Figure A.2 illustrates user profile use cases related to management of user profiles as an extension of some existing TISPAN Subscription Management (SuM) use cases [7].

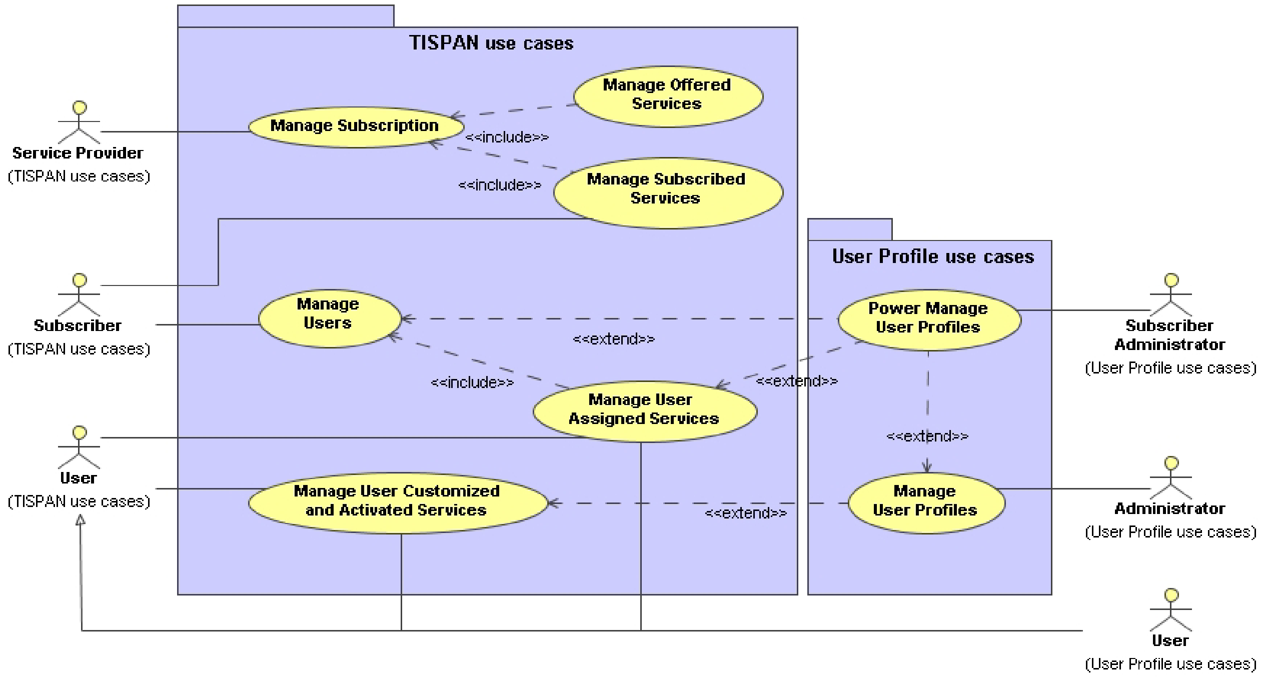

TISPAN use cases
User Profile use cases
Manage Subscription
Manage Offered Services
Manage Subscribed Services
<<include>>
<<include>>
Manage Users
Manage User Assigned Services
Manage User Customized and Activated Services
Power Manage User Profiles
Manage User Profiles
<<extend>>
<<extend>>
<<extend>>
<<extend>>
<<include>>
Service Provider (TISPAN use cases)
Subscriber (TISPAN use cases)
User (TISPAN use cases)
Subscriber Administrator (User Profile use cases)
Administrator (User Profile use cases)
User (User Profile use cases)

Figure A.2: User profile use cases as an extension of the SuM use cases

NOTE 1: The left side of the diagram represents existing TISPAN roles and use cases; the right side represents user profile roles and use cases.

NOTE 2: In figure A.2, the term "customized" is used, which is the TISPAN terminology meaning the same as "personalized" in the present document.

In figure A.2, "power manage user profiles " use case extends the "Manage User Profiles" use case and adds the ability to manage features which can be managed only by a user profile administrator who is also a service subscriber.

A.1.2 Common Profile Storage (CPS) defined in TR 132 808

The outline for a Common Profile Storage (CPS) function for PLMNs is provided in TR 132 808 [i.2] but has not been formally endorsed within ETSI TISPAN for the NGN. The scope of TR 132 808 [i.2] identifies that the driving aim of the study into CPS is to consolidate and co-ordinate the existing spread of databases to prevent redundancy and possible contradiction and to enable operators to administer and provision complex and combined services. The scope of the study documented in TR 132 808 [i.2] has been driven from the needs of Network Elements (e.g. MMS-RS, HLR, HSS, BM-SC); and from the needs of services/features including Service Management, Subscription Management and Charging Management.

A.1.3 3GPP Generic User Profile (GUP) Release 8 architecture

The Generic User Profile Release 8 architecture is described in [i.15]. Functional entities include:

Generic User Profile (GUP) Server: the GUP Server (GUPS) is a functional entity providing a single point of access to the Generic User Profile data of a particular subscriber. The GUPS includes the following main functionalities [i.15]:

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

In proxy mode, the application (named GUP Requestor, GUP R) requests user related data located in the GUP Data Repositories from the GUPS. After taking care of needed actions specified for the GUP S (and depending on the type of the request) the GUPS makes requests to the corresponding GUP Data Repositories and receives responses from them. Finally the GUPR gets a response to the original request from the GUPS. Depending on the type of the request also possible subsequent responses are delivered through the GUPS. In redirect mode the GUPR requests user related data located in the GUP Data Repositories from the GUPS. After taking care of needed actions specified for the GUPS (and depending on the type of the request) the GUPS returns to the requestor the information (e.g. address of GUP Data Repository(s)) to allow the GUPR to request the information from the GUP Data Repositories. The GUPR then directly requests the information from the GUP Data Repositories.

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

GUP Data Repository: Each GUP Data Repository stores the primary master copy of one or several profile components. The RAF provides for the standardized access to the GUP Data Repository. The storage formats or the interface between the RAF and GUP Data Repository are not specified by GUP.

Reference points include:

Rg: This reference point shall allow applications to create, read, modify and delete any user profile data using the harmonized access interface. The GUPS 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 GUPS 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.

Rp: This reference point shall allow the GUPS or GUPR, excluding external applications (e.g. located in a third party application or in the UE), to create, read, modify and delete user profile data using the harmonized access interface. Rp is an intra-operator reference point. External applications and third party GUP Data Repositories shall be connected to the GUPS only using the Rg reference point. The reference point Rp carries user related data, and therefore shall be protected by security mechanisms.

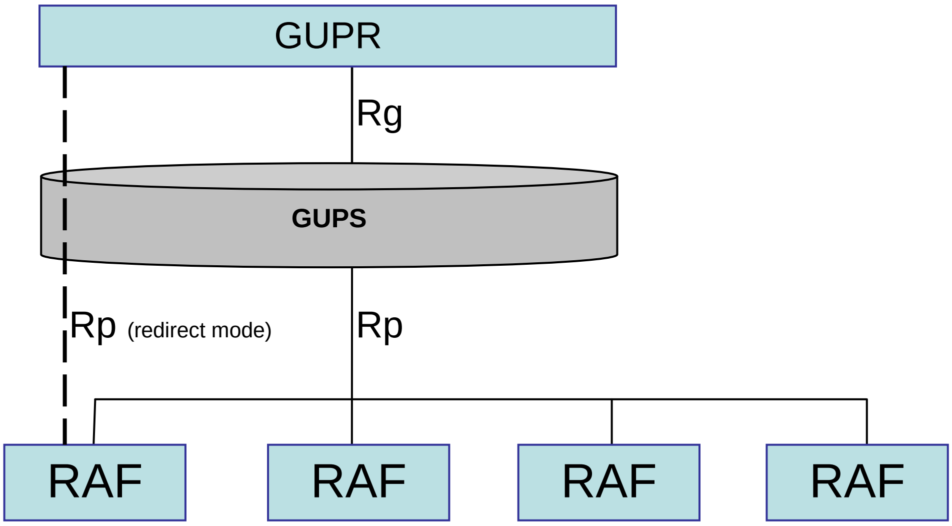


Figure A.3: 3GPP GUP architecture

A.1.4 Relationship to UPM distribution and synchronization capabilities

The CPS and 3GPP GUP Release 8 architecture described in clauses A.1.2 and A.1.3 are both examples of the approaches that may be use to meet the distribution and synchronization capabilities specified in clause 5.4.2 of the present document - particularly for profile components distributed amongst NGN network elements.

A.1.5 Universal Communications Identifier

The Universal Communications Identifier (UCI) concept [i.8], [i.9] evolved from a period when a user had many identifiers, covering many services but where each identifier was restricted to a single service, to the concepts now being developed in NGN where a single identifier, either a SIP URI or a Telephone number (E.164 [6] or tel-url), can be associated with many services. The UCI model was therefore a development based on the user-control of calls and sessions being separated from the network-provision of calls and sessions.

UCI offers a framework to allow user interaction with current and future user to user communications. Architecturally

UCI consists of two primary elements:

- Personal User Agent (PUA); and
- Service Agent (SA).

The various entities provided by the NGN, as already defined, are able to deliver a majority of the functionality that was specified in the UCI abstract architecture described in the earlier work on UCI (i.e. the Personal User Agent (PUA) and the Service Agent (SA) [i.32] functionality). The PUA is a functional entity that acts on behalf of the user within the communications network to manage communications based on user controlled preferences. The PUA is in a position to 'police' inbound communication and directs it to the device or media selected by the user based on user defined criteria.

The UCI architecture very broadly maps the Service Agent (SA) to the tele-services of ISDN-era telephony which of themselves map into the IMS/PES/PSS domains of the NGN. The Personal User Agent (PUA) maps largely into the application layer of NGN.

Reference points include:

Uu: Uu is a reference point allowing the UCI user to access the PUA.

The analysis of the use cases specified in [i.32] has led to the mapping of the UCI functional entities to NGN functional entities. Mapping the PUA reference points to NGN interfaces and/or internal reference points depends on its placement inside or outside the NGN environment as identified in [i.32]. Three scenarios have been identified:

- PUA is placed outside the NGN.
- PUA is placed inside the NGN as a new component.
- PUA is placed inside the NGN and is using the existing components. In this scenario, PUA represents a combination of UPSF, ASF, CSCF and NGN Presence Server.

Figure A.4 was included as figure 10 of [i.32] and shows the primary functional entities necessary to support UCI.

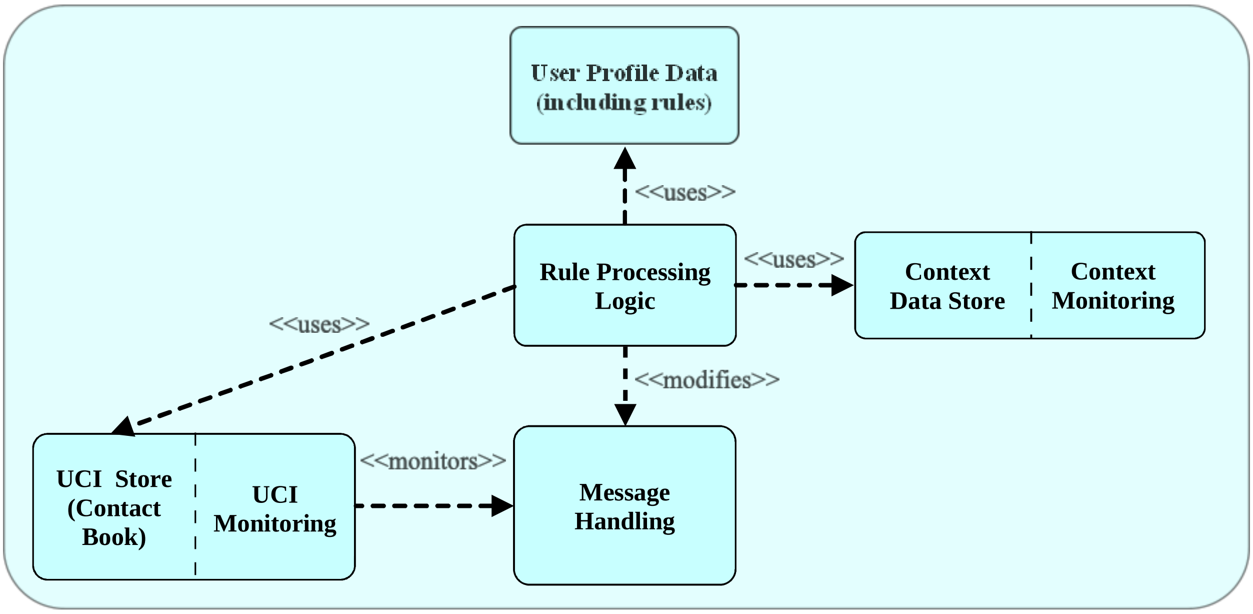


Figure A.4: UCI functional entities

The primary functional entity in figure A.4 that is specifically associated with the communication related functionality of UCI is the Message Handling block. In [i.32] it was identified that the PUA performed the control of communication sessions and extracted UCIs in SIP headers by inspection and modification of SIP headers of communication setup dialogs in which UCIs are used. To perform this function in an NGN requires Back-to-Back User Agent functionality (as identified in clause A.3 of [i.32]) and will, in TISPAN NGN map to the Call Session Control Function (CSCF). It is this functionality that is primarily represented by the Message Handling block in figure A.4.

What is clear from figure A.4 is that the functionality of the remaining functional entities matches very closely the functionality required in UPM. The Context Data Store, Context Monitoring and UCI Monitoring entities shown in figure A.4 can be seen to be capabilities that perform the role of the ContextProvider actor in the UseContextInformation use case of figure 5.1 of the present document. The functional entity "User Profile Data (including rules)" has a very direct link to the User-Profile object in UPM. The minimum profile necessary to deliver UCI may be seen as a subset of a broader based user profile that could be created from profile data specified in the present document. The "Rule Processing Logic" functional entity maps to the runRules method of the UPM User-Profile object [1]. The "UCI Store (Contact Book)" is merely a personal Address Book that contains UCIs (represented in UPM as a Group object whose members are Address-Book-Entry objects as defined in ES 202 746 [1]).

Annex B (informative): Core system objectives

These objectives were developed as core guidance for the development of the material in the main body of the present document and are provided as useful background for interested readers.

B.1 Stakeholder categories and their objectives

The main objectives of various stakeholder categories are:

- End-users: personalize their services and get the expected user experience. The user requirements of users are described in detail in EG 202 325 [i.1].
- Profile providers: providing means for end-users to define their preferences in their user profiles. It includes:
    - storing profile data;
    - synchronizing of profile data which may be stored in a range of locations such in the network, devices and services;
    - and making data available to the user and their services and devices which should be personalized.
- Network providers may:
    - provide services such as:
        - Storing and transporting of user profile data and service data;
        - Services such as synchronization of data, capability negotiation;
    - benefit from the user profiles as their services might be personalized.
- Regulator: there are regulations on a range of issues that may affect personalization, in particular for protecting the user regarding data sharing and confidentiality.
- Service and device providers:
    - personalize services and devices according to users' needs by retrieving data in the user profiles;
    - contribute to a better user profile by updating it according to user behaviour, if the user agrees. For example, if the user change settings in the service the service provider can suggest that the preference corresponding to the setting is updated in the use profile.

B.2 Management of user profile data

A large amount of data related to the users' services and devices and their preferences stored in their profiles will need to be:

- Created (mention data editing, e.g. creation templates update etc.).
- Stored: The data should be stored in a secure manner with user agreed levels of privacy applied to the availability and distribution of that data.
- Accessed: Ideally, profile data should always be available, over all networks, from all supported devices and services, including fixed and mobile services allowing service continuity and optimal user experience. The access control need to respect principles regarding user control and legal policies.

- Synchronized: Data at different locations should be kept consistent, which may be ensured by synchronization of data and transaction security. However, although the profile data (or copies of profile data) can be distributed amongst devices and services, it should be possible to ensure that users can have the concept of centralized profiles which cover all of their devices and services.
- Backed up.

B.3 Processing of profile data

The profile data needs to be processed, including:

- associating the UPM system with contexts including the users' services, devices and presence information;
- sharing data with related services, devices and other people;
- running rules defined by the user;
- providing service response to user preferences.

B.4 Activation/deactivation of situation profiles

Situation dependent profiles need to be activated and deactivated according to the users' activation rules. It will therefore be necessary that the system:

- acquires contextual information from presence and service/device status information (e.g. subscribe to state changes);
- runs activation rules.

B.5 Information and feedback to users

The users' need to feel in control of their profiles. It will therefore be necessary that the system:

- keeps the users' informed about their current services and devices in relation to their profiles;
- provides different amount of information depending on average/expert user and their individual preferences.

The system should inform the user:

- which situation profile(s) is/are active;
- whether a service support UPM.

B.6 Logging

The system should collect information related to a range of activities of the personalization system and store them in logs. The information in logs can be useful for various categories including end-users and system administrators. The following may be logged:

- changes to the profile data such as preference settings;
- activation and deactivation of profiles;
- rules applied;
- activities related to services and devices addressed in profiles.

Annex C (informative): Related Work in other Standardization Bodies

C.1 Open Mobile Alliance

The OMA User Agent Profile V2.0 Enabler [i.16] enables the end-to-end flow of a User Agent Profile (UAProf) between the device, the intermediate network points, and the origin server ensuring that the relevant device capability information is available for necessary parties. Origin servers, gateways, and proxies can then use the capability information to ensure that the user receives content that is particularly tailored for the environment in which it will be presented. Same as UAProf V1.1 with the addition that schemas are machine readable and thus profile validation can be automated.

The Device Profile Evolution (DPE) enabler [i.17] provides a standardized solution to convey information on the device capabilities. While other enablers such as UAProf can only convey information on static device capabilities, the DPE enabler can convey information either on static device capabilities or on dynamic device capabilities, the dynamic aspect being the main added-value of the DPE enabler.

OMA Device Management (DM) Working Group was formed by consolidating the device management activities taking place previously in the former WAP Forum and the former SyncML Initiative. The goal of the Device Management Working Group [i.18] is to specify protocols and mechanisms that achieve management of mobile devices including the necessary configuration to access services and management of the software on mobile devices. OMA Device Management (DM) is a technology allowing remote entities to monitor and configure mobile devices on behalf of the end user. The remote entity is called management authority and can be a wireless operator, a service provider, a customer care or other kinds of remote device administrator. The management authority interface with a server located in the operator's network. There are several use cases possible for DM technology, among which: initial configuration of a device, changes to settings and parameters, enabling or disabling features, software upgrades, remote procedure execution, fault management. However, not all these features are mandatory for the protocol and according to DM specification, so devices may optionally implement all or a subset of them. In the context of 3GPP GUP [i.15], DM technology has been chosen as an alternative to having a Repository Access Function inside the end user equipment, as DM allows remote managing of device configuration in an efficient way, especially optimized for wireless and cellular connections.

OMA DM protocol [i.19] is a request response protocol, involving a DM Client (embedded in the device), and a DM Server. The communication is initiated asynchronously by the DM Server. The protocol is abstract and can be implemented through several different transport mechanisms, including WAP push, SMS, or other means. Security is taken in account using a built in authentication in the protocol, thus to avoid unauthorized entity to perform malicious operations on the device. Other than request-response exchanges, OMA DM defines alerts, i.e. messages that can occur out of sequence, and can be initiated by either the DM Server or the DM Client. Alerts are used to handle errors or abnormal terminations, report on device performances, etc.

OMA XML Document Management [i.20] defines an architecture and a protocol to allow an XDM client (a UE or an AS) to handle information stored in various network repositories in form of XML documents. XDM is the supporting technology for accessing and manipulating data coming from different communication services related to applications such as Presence [i.21] [i.22], Push to Talk Over Cellular (PoC) [3], Instant Messaging (IM) [i.23], etc. XDM specifications [i.24] have been endorsed by TISPAN [i.25]. XML Document Management Architecture - Candidate Version 2.1. [i.26] extends the previous specifications and introduces distribution across different networks in order to extend the management of documents also to documents residing in other network domains. In addition, it defines interface to implement charging.

The following topics are in the scope of XDM specifications:

1) A HTTP based interface for describing elements and attributes of an XML document as HTTP resources accessible via HTTP URIs.

2) A technique for using HTTP GET, PUT and DELETE methods for various document manipulation operations such as creating, retrieving or deleting elements and attributes (adapted from the IETF XML Configuration Access Protocol (XCAP) [i.27]).

3) A SIP-based interface which can be used to convey changes in XML documents to an XCAP client, provided that the client has subscribed to receive such changes.

4) A subset of Xquery [i.28] (Limited Xquery) to be used over HTTP interface, which extends the range of operations on XML documents provided by the legacy XCAP interface.

5) A network-to-network interface to enable search of information across XDMS of multiple domains and retrieval of a document from the remote network.

C.2 W3C

In former years, W3C has produced several specifications allowing a user agent to exchange profile and context information with a remote entity. Mainly, these specifications make use of semantic languages which W3C itself has previously defined, like RDF and OWL.

W3C CC/PP [i.29] uses W3C Resource Description Framework (RDF) to create profiles and extendible profile schemas that describe user agent capabilities and preferences. A CC/PP profile contains one or more components, and each component contains one or more attributes. To describe client capabilities and preferences, the client being described is identified as a resource whose features are described by labelled graph edges from that resource to corresponding object values. The graph edge labels identify the client feature (CC/PP attribute) being described, and the corresponding object values are the feature values. Attribute names are URIs, with XML namespace syntax used to avoid some of the RDF expressions becoming too cumbersome. All simple attributes are represented by RDF typed literal values, and attributes that need to have multiple values use sets or sequences. Default attribute values are externally defined and are referenced from within each component. The most known application of W3C CC/PP is OMA User Agent Profile (see clause C.1).

W3C Mobile Web Initiative - Device Description Working Group has produced the Device Description Repository Core Vocabulary [i.30] using W3C Delivery Context Ontology (DCO) [i.31], which provides a formal model of the characteristics of the environment in which devices interact with the Web. Each class in DCO is associated with a set of properties. These properties are defined in tables in the appropriate section of the specification. Each row in a table defines single property in terms of a number of facets like name, type (can be data types or classes, classes being themselves defined in the same or in another ontology), description, occurs (the cardinality of the property), values (values that apply across every instance of a class, similar to constants), alternate names.

Annex D (informative): Security terms and concepts

D.1 Security associations

The detail design of security in the context of UPM (and user profiles in general) requires consideration of the security associations between objects, i.e. those relationships between objects that are open to attack and which are protected by the provisions of the architecture. Such associations exhibit a number of properties with respect to security and have to be considered in the overall design. Security associations are:

- Links that determine assurance.
- Links that determine security functionality.

A security association defines:

- Algorithms used for each security capability.
- What security capabilities are available.
- What keys are to be used.

D.2 Confidentiality

The aim of confidentiality measures are to ensure that communication between Alice and Bob, if intercepted by Eve, remains confidential. In other words Eve cannot access the content of the communication.

D.3 Integrity

The aim of integrity measures is to provide assurance that text has not been modified.

The method of operation of an integrity protection and validation mechanism generally involves the following steps:

- Prepare a digest of the text at source.
- Prepare a digest of the text at the destination.
- Compare it to a digest of the text calculated at the destination.

If the digests are the same there is a high assurance that there has been no manipulation of the text in transit. The aim of any cryptographic algorithm for integrity is to give assurance that the integrity check sum can only be generated from the original text and that any change in the text will result in a different integrity check sum (i.e. relies on inability of attacker to create a matching check value with random tools and data).

D.4 Authenticity

The aim of authenticity measures are to prove that Ann is really Ann with the intention to make it difficult for Bob to masquerade as Ann. The person or entity being authenticated is termed the Principal and authentication methods rely upon something that the Principal **is**, **has** or **knows**

- Is = Biometric data.
- Has = Token, smartcard.
- Knows = Password.

This is sometimes supplemented by how the principal does things (behaviour). The methods of achieving authentication fall into two root classes (for cryptographic authentication):

- Challenge - response
  - The authenticator challenges the authenticatee, who responds, and the authenticator checks the response. The method relies on inability of an attacker to guess the correct response even with knowledge of the challenge and the algorithm used to generate the response.
- Keyed digest
  - Process some data using tools only the transmitter should have to give a summary, send it. If the receiver can only match the summary using matching tools then it was created and sent by the transmitter. Relies on inability of attacker to create a match with random tools and data.

D.5 Authority

Authority is the ability to answer the question "is Anne allowed to that?" where "allowed" is a statement of Anne's authority. In many computer systems files have attributes of Read, Write, Delete (and others) and the rights of the user determine which of these capabilities are available to each user. In a more distributed environment such as in telecommunications the assertions of authority are more complex and require some form of Authority Management Infrastructure (AMI) which can be found in two main suites of protocols and objects:

- Security Assertion Markup Language (SAML).
- Privilege Management Infrastructure (PMI) in X.509 Attribute Certificates.

For both SAML and PMI authority, and its validation, may be described as follows:

- Authority A was issued at time t by issuer R regarding subject S provided conditions C are valid.

A pre-requisite of authority validation is authentication, and that itself has a pre-requisite of identification.

Annex E (informative): Conflict resolution/avoidance

E.1 Priorities for avoiding conflicts

Potential conflicts may appear when two (or more) Scope objects that are associated with the same profile data are simultaneously active, as they both potentially define the attributes of that profile data in the active profile. The system needs to determine which of these alternative values is to be applied in the active profile.

In order to avoid conflicts, priorities will be assigned to Scope objects. Groups of profile data (represented to the user as a "situation profile") can be associated with the same Scope object, thereby acquiring the same priority. It is also possible that individual profile data within the same situation profile can have a higher priority by being associated to a Scope object with a higher priority but with the same activation conditions. In all cases, the attributes of the profile data that are set in the active profile will be those associated with the Scope object with the highest priority.

The "Normal" Scope object is assigned the priority "0", whereas all other Scope objects have a higher priority. This ensures that when a user defined "situation" occurs, the attributes of the profile data in the active will be set to those in the Profile-Item-Attributes object associated with the Scope object that relates to that situation.

Priorities can be defined by the profile administrator. General situation profiles will be associated with a Scope object with a priority in the range 1 to 5 (decimal values). It is expected that eHealth profiles will be allocated higher priorities than non-eHealth profiles. The highest priority is reserved for Emergency profiles.

It is advisable that profile providers should assist users in defining priorities to avoid potential conflicts.

E.2 Avoiding conflicts by using templates

Potential conflicts (when profile data items are associated with two or more active Scope objects with the same priority), may be resolved by the use of a well designed set of pre-defined profile templates that assign priorities to profile data in a way that eliminates conflicts for most probable combinations of situations that would be likely to occur.

It would be expected that if profile administrators create their profiles by utilising a "creation wizard", the wizard would make use of such a coherent set of templates and would thus create an initial profile setup where conflicts are eliminated or confined to extremely unlikely combinations of situations.

If administrators create their own profiles without using the templates, or if they amend the priorities of profile data in profiles that are created from these templates (by reassigning the priorities of Scope objects), then they may introduce future potential conflicts. This may also occur whenever the chosen combination of templates is not consistent.

E.3 Conflict resolution/avoidance methods

The methods described in this clause can be considered as part of Special Resolution Policy referred to in clause 5.4.4. They are suggested methods for avoiding the creation of ambiguous states in the operation of a UPM system. However, profile providers are free to choose other methods than those described, particularly if they produce a better user experience for the profile user.

E.3.1 Method 1

Method1 is suitable for use at profile creation or update time. This method consists of identifying possible conflicts whenever a profile is created or updated.

When a profile is created or updated then:

1) The system identifies which profile data have associated Scope objects with the same priority but with at least one attribute of the associated Profile-Item-Attributes objects having different values.

2) Assisted by the system, the profile administrator can be asked to consider:

   - modifying the conflicting attributes in the Profile-Item-Attributes object to remove the conflicts (this option will create no further conflicts);
   - disassociate the profile data item from one or more of the Scope objects by deleting one of the conflicting Profile-Data-Item-Attributes objects (this option will create no further conflicts);
   - modify the priorities of one or more of the Scope objects (this may create different conflicts in other profile data associated with the Scope object and could lead to a complex and unpredictable cycle of updating).

The above processes, if fully and successfully completed, should eliminate the risks of conflicts occurring during normal operation of a user's profile. However, if dynamic updating of profiles occurs during normal usage, additional conflict situations may be introduced.

This ranking procedure is only recommended for use at profile creation time in order to avoid disturbing the person when a conflict arises in an inappropriate situation (e.g. when the person is busy or using a device which is not convenient for managing profiles).

E.3.2 Method 2

Method 2 is suitable for use during normal operation as well as during profile creation or update. This method consists of explicitly asking users to choose their preferred value in a given situation. This could be achieved either by presenting options for the user to select or by capturing a setting that the user makes in the user interface of a device or service. The user choice is then recorded and permanently associated to a new Scope object that characterises this specific situation.

E.3.3 Comparing conflict resolution methods

Potential conflicts are often best resolved when the user has time to deal with them and ideally with a sufficiently large screen (rather than being asked in any situation). It is therefore recommended to avoid future potential conflicts by assigning priorities at creation time.

Conflict resolution method 1 is suitable for use at profile creation time. Method 2 is suitable for use during profile creation or update (conflict avoidance) and during normal usage (conflict resolution). However, the user may not wish to deal with any conflict resolution during normal usage of their devices and services. In that case, a conflict resolution process that does not require user intervention can be chosen, as explained in clause E.3.5 on "Conflict resolution without user involvement".

E.3.4 User choices of handling conflicts at run-time

When a conflict is detected at run-time, there are alternative ways to handle it. The user may be asked to choose among different options affecting the value of the profile data as described in clause E.3.2. The conflict may occur in a situation when the user might be busy or when they using a device that does not make it easy to handle such conflicts.

The degree of involvement of the user in the resolution of the conflict would be decided during initial set-up of the user profile management system and could subsequently be amended by the user at a later date. Typical options for such a rule, as expressed to the user, are:

- "When the conflict occurs, ask me".
- "At a later stage, when I am not busy, ask me".
- "Do not care, keep the current value without changing it" (in this case the "current value" is the value of the profile data item before the Scope that is causing the conflict was activated).

E.3.5 Conflict resolution without user involvement

If users do not wish to be involved in actively handling profile conflicts, then an alternative automatic resolution process should be provided to ensure that a resolution is made.

E.3.6 Method for capturing and utilizing the results of a resolution process

When a conflict resolution involving Scope object A and Scope object B (or more Scope objects) is triggered, and a resolution process has been completed, the result of the resolution process should be stored in a new Scope object (named Scope object A&B). Scope object A&B should have a priority that is higher than either Scope object A or Scope object B. The context Evaluation method [1] of the new Scope object would contain an activation condition that is a merge of the activation conditions of Scope object A and Scope object B.

Annex F (informative): Analysis of candidate protocols and mechanisms for UP/UPM security provision

F.1 Overview

One of the main cryptographic concerns in any system is the choice of keying management infrastructure. Where the set of security associations is very small (1 ideally) then symmetric key associations are most common and can be used successfully. However where a large number of associations need to be created and maintained for varying lengths of time an asymmetric association model is more commonly considered.

F.1.1 Symmetric key solutions

In symmetric solutions the two communicating parties share a single secret and are the only parties who know the secret. Such solutions are commonly used in cellular radio (GSM, UMTS) and are primarily used to provide authentication and to derive a key for confidentiality of communication.

F.1.2 Asymmetric key solutions

The technology of asymmetric key cryptology has its roots in a thought paper from Ellis of the UK wherein he proposed a means to offer confidentiality without the need to exchange secrets. The resultant mathematical models form a key in two parts one of which can be made public and one of which remains private (i.e. never shared with anyone). In practical implementations, exemplified in the X.509 model aligned with the X.500 directory, the public component is certified by a trusted third party as belonging to a specific person and that the private key component exists. This party certifies this and is known as a certification authority. Public key models allow control of authenticity and may be used in providing confidentiality and integrity.

F.2 Authorisation Single-Sign On approaches

Single Sign On is a collective description in which a single login/registration to a system enables access to the suite of services available to the user. For example logging onto a network may allow access to email servers, application servers, print servers and so on that may each require authentication. SSO mechanisms allow the initial sign-on to enforce the authentication through authorization across the suite of servers that make up the system and prevents the user requiring to uniquely authenticate to each resource (e.g. printer server).

F.2.1 Generic Authentication Architecture (GAA)

The purpose of GAA is to provide support for security features and mechanisms to allow authentication and key agreement for application security by extension of the 3GPP AKA mechanism. Although not specified in detail the applications that may use GAA, and its bootstrapping architecture GBA, include but are not restricted to subscriber certificate distribution as defined in TS 133 221 [4]. The intent of subscriber certificates in the context of GAA and GBA is to allow support of services either provided by the CSP, or in whose provision the CSP is a partner.

F.2.2 X.509 Privilege Management Infrastructure (PMI)

The initial role of X.509 [i.14] was to define the use of public key certificates for the authentication of entries in the X.500 directory. The extension for access control is achieved in X.509 by the use of Attribute Certificates (AC) within a Privilege Management Infrastructure (PMI) that enables privileges to be allocated, delegated, revoked and withdrawn in a secure way against system components or operations (resources). In most instances the PMI provides authorization after authentication has taken place.

NOTE: A PMI for authorization is analogous to a Public Key Infrastructure (PKI) for authentication and thus may exist alongside an X.509 based PKI for authentication.

In mapping X.509 PMI to UP/UPM an attribute certificate is defined to be associated with a particular UP/UPM capability (or set of capabilities) such as "access address book", or "synchronise profile" or resource (the profile).

The PMI model introduces a number of entities to the architecture:

- Source of Authority (SOA):
  - The root of trust of a PMI. This is an entity that a resource implicitly trusts to allocate privileges and access rights to it.
- Attribute Authority (AA):
  - An entity delegated to act on behalf of the source of authority.
- Privilege asserter:
  - The entity asking for access to a protected resource.
- Privilege Verifier:
  - The privilege verifier needs to have access to the following information before it can verify any claimed privileges:
    - the public key of the trusted root CA (this has to be configured into the verifier by some trusted means) so that it can verify signatures on the ACs and PKCs that it will evaluate;
    - the name and public key of a trusted SOA, either configured into the verifier by some trusted means or via a public key certificate that can be validated against the root CA's public key, so that the verifier can validate that ACs are issued directly or indirectly by this SOA;
    - the policy rules that direct how the verifier can determine that the presented privileges are "sufficient" to access the resource, and how to determine that delegated privileges are less than held privileges (these have to be configured in by some trusted means);
    - any local variables used in verifying the claimed privilege e.g. time of day. Again these have to be configured in by some trusted means;
    - the attribute certificates of the privilege holder, plus a valid chain back to the SOA, plus the latest revocation information. This information may be obtained from the holder and/or a public directory service. Since the data is digitally signed it cannot be tampered with without detection and therefore does not need to be configured in by trusted means.

Whilst PMI introduces a number of access control models (Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC)) the scheme for verifying the privileges is identical in each case.

The X.509 Attribute Certificate (AC) strongly binds a set of attributes to its holder, and these attributes are used to describe the various privileges that the issuer has bestowed upon the holder. The issuer is termed an Attribute Authority (AA), since it is the authoritative provider of the attributes given to the holder. The whole data construct is digitally signed by the AA, thereby providing data integrity and authentication of the issuer. Each AC contains details of the holder, the issuer, the algorithms used in creating the signature on the AC, the AC validity time and various optional extensions. Because the AC is digitally signed by the issuer, then any process in possession of an AC can check its integrity by checking the digital signature on the AC.

F.2.3 XDM for Access Control

XDM refers to the schema for User Profiles defined using XML by the OMA. The schema offers a number of services related to the use of access rights and these are summarised below:

- Pre-requisites:
  - XDM clients is expected to have been authenticated before accessing any XDM services.
- Operation:
  - The Aggregation Proxy upon receipt of a request from a Search Proxy in a trusted network authorises access to its XDMS and uses TLS or other mechanisms to allow secure data transfer.

NOTE 1: An XDM client located in an UE is authenticated by the Aggregation Proxy.

NOTE 2: An XDM client located in an AS is authenticated directly by the XDM server.
XDM search proxy (used for implementing distribution) is expected to have been authenticated as described by the XDM specification.

NOTE 3: The HTTP Digest scheme is the default authentication mechanism assumed for XDM although HTTP Digest is generally considered a weak authentication scheme in overall security terms. In order to provide integrity and confidentiality protection to the exchanged messages TLS is used.

NOTE 4: The XDM specifications given in the OMA Push to Talk over Cellular Architecture [3] define a default access control policy in which only the creator of a document is allowed to perform all XDM actions to the document, and application servers of the trusted networks are allowed to read the document with all other access denied.

F.2.4 Kerberos

Kerberos is one of a family of distributed authorization mechanisms that allow for Single Sign On (SSO) to be performed. Kerberos manages the relationship between clients and servers without the client having to have a predefined security association with the server. The Kerberos model has a centralized key distribution centre consisting of an authentication server (AS) and a Ticket Granting Server (TGS), and on the outside a client and a service server (SS). The client authenticates itself to AS, then demonstrates to the TGS that it's authorized to receive a ticket for a service (and receives it), then demonstrates to the SS that it has been approved to receive the service.

Kerberos may be considered as a symmetric key variation of the X.509 PMI described in clause F.1.2.

History

Document history		
V1.1.1	December 2009	Publication