ETSI EG 284 004 V1.1.2 (2007-09)

ETSI Guide

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)

Reference
DEG/TISPAN-04004-UCI

Keywords
security, SIP, UCI

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

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 ETSI Guide (EG) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

UCI has been developed over a number of years within ETSI. When development of UCI was started it began as a means to counter the problems that users perceive when their phone number, email addresses and other electronic identifiers change over time. A single global identifier for the user was conceived but with a view to reflect a desire on behalf of users to manage the ever-richening capabilities of their electronic communications world. As such UCI has evolved to serve as a model for user-control of a rich and diversified communications network. One of the early keys in the UCI development was to model a separation of the user controlled parts of the communication from the nitty-gritty network and services of a communication network. In this way was conceived a "Personal User Agent" (PUA) that acted on behalf of the user within the communications network to manage communications based on user controlled preferences. The PUA would be in a position to 'police' inbound communication and direct it to the device or media selected by the user based on user defined criteria. The actual communication was then conceived to be handed off to a "System Agent" or "Service Agent" that actually dealt with the detail of network and protocols to serve the user's preferences.

Within the NGN as defined in ETSI TISPAN the time is now ripe to introduce UCI. There are a number of design decisions made for the NGN that ease the adoption significantly. Foremost of these is that the NGN is IP based and therefore can build upon the set of technologies familiar from "The Internet" including future web-based-services. The use of SIP and SDP as key protocols in the NGN also aid greatly in facilitating wide sets of media rich services with a common protocol set. The abstract nature of the IP protocol suite and the use of its key resolution protocols (DNS and ENUM) serve to allow many of the retained identity features key to UCI.

1 Scope

The present document identifies approaches to incorporating UCI capabilities as defined in EG 202 067 [2] and EG 203 072 [3] into ETSI's TISPAN NGN. The present document provides a review and assessment as to what extent existing standards, specifications and guidelines support elements of a UCI implementation and how, if necessary, they should be adapted in order to more fully support complete UCI implementation. The analysis presented is not restricted to only those standards and specifications developed in TISPAN but also covers the work of other bodies (whose work is already being incorporated to the NGN):

- a review of the work done by Liberty Alliance in this area is provided in annex C;
- a review of the existing TISPAN NGN capabilities to provide a UCI presence service is provided in annex B; and
- a review of SIP capabilities in this area is provided in annex A.

An outline abstract model of UCI showing use-cases, architecture and information flows is given in clause 5 and an analysis of how existing NGN protocols and capabilities support them is given in clause 6. The abstract model shows how the UCI elements are carried and how they may be presented across the NGN.

The present document provides, in clause 11, a model showing how UCI exists in the context of other developing standards work at ETSI and how they fit to the existing NGN model.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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.

[1] ETSI EG 201 940: "Human Factors (HF); User Identification solutions in converging networks".

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

[3] 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".

[4] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[5] IETF RFC 3261: "SIP: Session Initiation Protocol".

[6] Void.

[7] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[8] ETSI TS 183 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); Protocol specifications".

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

[10] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive - OJ L 108, 24.04.2002).

[11] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive - OJ L 108, 24.04.2002).

[12] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive - OJ L 108, 24.04.2002).

[13] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - OJ L 108, 24.04.2002).

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications - OJ L 201, 31.07.2002).

[15] Void.

[16] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat and Risk Analysis".

[17] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[18] ETSI TS 122 141: "Universal Mobile Telecommunications System (UMTS); Presence service; Stage 1 (3GPP TS 22.141 version 7.0.0 Release 7)".

[19] ETSI TS 123 141: "Universal Mobile Telecommunications System (UMTS); Presence service; Architecture and functional description; Stage 2 (3GPP TS 23.141 version 7.2.0 Release 7)".

[20] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

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

[22] IETF RFC 2327: "SDP: Session Description Protocol".

[23] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (Data Protection Directive - OJ L 24, 30.01.1998).

[24] IETF RFC 3856: "A Presence Event Package for the Session Initiation Protocol (SIP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 203 072 [3] and TR 180 000 apply.

3.2 Abbreviations

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

AoR	Address of Record
AS	Application Service
ASF	Application Server Function
BGCF	Border Gateway Control Function
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	Connected Line Identification Presentation
CSCF	Call Session Control Function
CSP	Communications Service Provider
DNS	Domain Name System
ECN	Electronic Communications Network
FFS	For Further Study
IBCF	Interconnection Border Control Function
I-CSCF	Intermediate-CSCF
ID-FF	Identity Federation Framework
IdP	Identity Provider
IMS	IP Multimedia System
ISC	IMS Service Control
ISDN	Integrated Services Digital Network
IWF	Inter-Working Function
ID-WSF	Identity Web Services Framework
LECP	Liberty-Enabled Client or Proxy
MGCF	Media Gateway Control Function
NGN	Next Generation Network
NNA	Naming Numbering and Addressing
OASIS	Organization for the Advancement of Structured Information Standards
PDA	Personal Digital Assistant
PES	PSTN Emulation (Sub)System
PSS	PSTN Simulation (Sub)System
PSTN	Public Switched Telephone Network
PUA	Personal User Agent
SA	Service Agent
SAML	Security Assertion Markup Language
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SP	Service Provider
UCI	Universal Communications Identifier
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
UTF-8	Unicode Transformation Format-8
XML	Extensible Markup Language

4 Summary of UCI in NGN analysis

The UCI concept has evolved from a period when a user had many identitifiers, 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 [9] 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.

NOTE 1: The use of the terms identity and identifier in the present document refer only to the means to identity a user of services from the NGN and does not confer any legal status that contradicts the identity of a person or entity as a legal entity.

The primary characteristics of the UCI as an Identifier, rather than as a system which is covered later in the present document, is that there is one element that is authoritative and can be proven to be unique within the operational area (which may be global, regional, national or corporate). The analysis undertaken in EG 203 072 [3], identified that the authoritative element, called the UCI-numeric part, should be drawn from the E.164 [9] format and have similar controls. The analysis presented in the remainder of the present document shows that the management of the SIP URI as proposed in TISPAN's NGN provides an ideal method to support UCI. It can be shown that the requirement of authority and the ability to associate service, labels and aliases suggest that SIP, in its extended NGN format, can meet almost all of the identity requirements of UCI. If the UCI-numeric part is also made publicly available for use and placed into ENUM (where ENUM provides the resolution service), the remaining requirements related to UCI can also be met.

NOTE 2: If SIP URIs are selected in the NGN to play the role of the UCI-numeric part then it is fair to note that the element name UCI-numeric is inaccurate.

The various entities provided by the NGN, as already defined, are able to deliver the majority the functionality that was specified in the UCI abstract architecture described in the earlier work on UCI (i.e. the Personal User Agent and the Service Agent functionality). Delivering all of the required functionality could be achieved by either making small extensions to the already described NGN capabilities or by the use of an additional entity that manages those extra functionalities This extra functionality could be considered as an enhancement to a basic level of UCI capability and hence systems without that additional functionality could be created with little or no increase to existing NGN capabilities. Certainly, there is no hard and fast requirement to maintain the separation of Personal User Agent and Service Agent just to maintain the UCI model if they have been adequately taken over in the NGN. Similarly the conceptual reference points proposed in UCI do not need to be maintained if they can be shown to be mapped to the NGN.

The UCI architecture therefore abstracts the user-management of communication (e.g. intrusion) in the Personal User Agent, from the nitty-gritty network management of sessions in the Service Agent. The former is user-centric, the latter is not. Further analysis of the UCI model, beyond that done in the earlier work EG 201 940 [1], EG 202 067 [2], EG 203 072 [3], has clarified a number of functional components that a PUA requires in order to deliver the functionality described in the various scenarios discussed in the earlier work (see annex A). From this clarified model of the functional components of a PUA it has been possible to identify clear mappings to a number of NGN components (see annex A). This mapping shows a very strong alignment between the PUA functional components and the NGN components.

As the NGN defines clear protocols and behaviours for interaction between all of the different NGN components, it follows that those PUA components that are clearly mapped to NGN components will also be supported with protocols and behaviours that will provide substantial support for UCI. Those PUA components that are not clearly mapped to appropriate NGN components have been mapped to a single PUA Application Server (AS). As the allocation of ASs to a SIP session is provided for within the basic operational model for the NGN, the allocation of the AS needed to complete the PUA functionality should also be fully supported by the NGN.

Annex A indicates the functionality that will need to be added to the NGN, as part of a PUA Application Server, in order to perform the more sophisticated functions of a PUA. However, the precise way and extent to which these functions are implemented is outside the scope of TISPAN specifications, as is the general case for ASs.

The analysis presented above identifies a number of reasons, backed up by analyses in the remainder of the document, that suggest UCI is available in the NGN. The only significant barrier to the UCI capability suite as defined in previous ETSI documents is the commercial adoption of the user-centric services offered by UCI on top of the existing NGN model.

Table 1 summarizes the analysis of how the UCI as an identifier maps to the SIP protocol data elements. Once again it is possible to summarize this as there being no requirement to add information elements in SIP solely for the purpose of UCI.

Table 1: Mapping between UCI-identity-elements and SIP data elements

UCI element	SIP element	Notes and observations
UCI-numeric (see note)	The UCI-numeric for the originator of the request will be the username part of the UCI user's AoR. It will thus appear as part of the From field. The UCI-numeric of the target user will appear as the username part of the Request URI and the URI in the To field.	The realm element of the Request URI and the To field will either be the valid realm of the target user or a dummy realm that the originating user's PUA will recognize and re-write into the valid realm for the target user. E.g. <UCI-numeric>@re-write-me.com Also, the username element of URIs using this dummy realm may be nicknames that the originating user's PUA will re-write into the UCI-numeric associated with that nickname. This is directly analogous to the use of dummy realms to support anonymous communication as specified in clause 8.1.1.3 of RFC 3261 [5].
	Request URI, To Field and From field.	The SIP URI of the request originator appears in the From field and the SIP URI of the target appears as the request URI in the To field. The user field of each of these SIP URIs will contain the appropriate UCI-numeric.
UCI-label	User-specified, session specific, UCI-label information may precede the URI in the From field.	The UCI user may choose to specify a label that they wish to use for this session, in which case this should precede the URI in the To field. Otherwise, nothing should precede this URI. The UCI user's PUA will know from its internal rulebase which of the UCI-user's pre-defined set of labels to use in its subsequent transactions with other PUAs.
	From field.	The UCI-label of the request originator may appear before the SIP URI in the From field.
UCI- AdditionalData	This should appear as part of the message body of the request.	The format and content-type descriptions for the message body are FFS.
		The format and content-type descriptions for the message body are FFS. One element of the additional data will indicate whether the label that follows the SIP URI in the From field is an authentic UCI-label for that user.
NOTE: For the UCI-numeric mapping in the NGN either SIP-uri or E.164 in a tel-uri may be selected.		

Finally in this summary table 2 considers the mapping of SIP header content to UCI and again finds no missing elements that would have to be added before allowing NGN to support UCI.

Table 2: SIP header content mapping to UCI fields

SIP Header name	SIP content	UCI mapping
Via	The address at which Alice is expecting to receive responses to this request. It also contains a branch parameter that identifies this transaction.	No special UCI mappings.
To	A display name (Bob). A SIP or SIPS URI towards which the request was originally directed.	When the User B is a UCI user, the SIP URI is their UCI SIP URI. The display name used may have no relationship with any variant of User B's UCI-label.
From	A display name (Alice) and, A SIP or SIPS URI (sip:alice@atlanta.com) that indicates the originator of the request. A tag parameter containing a random string (1928301774) that was added to the URI by the softphone. It is used for identification purposes.	For all requests sent from User A's PUA, the display name will be a UCI-label associated with User A's UCI.
Call-ID	A globally unique identifier for this call, generated by the combination of a random string and the softphone's host name or IP address.	No special UCI mappings.
CSeq or Command Sequence	An integer and a method name. The CSeq number is incremented for each new request within a dialog and is a traditional sequence number.	No special UCI mappings.
Contact	A SIP or SIPS URI that represents a direct route to contact Alice, usually composed of a username at a fully qualified domain name (FQDN). While an FQDN is preferred, many end systems do not have registered domain names, so IP addresses are permitted.	No special UCI mappings.
Max-Forwards	An integer that is decremented by one at each hop.	No special UCI mappings.
Content-Type	Contains a description of the message body	No special UCI mappings.
Content-Length	Integer. Contains an octet count of the message body.	No special UCI mappings.
NOTE 1: While the Via header field tells other elements where to send the response, the Contact header field tells other elements where to send future requests. NOTE 2: The combination of the To tag, From tag, and Call-ID completely defines a peer-to-peer SIP relationship between Alice and Bob and is referred to as a dialog.		

5 UCI review and TISPAN capabilities

5.1 UCI review

5.1.1 UCI Rationale

In almost all current identification schemes, there is an attempt to have a single identifier perform (at least) two different functions, namely:

a) to identify end-points in such a way that the identifier can be processed by information and communication systems to enable end-to-end service instances between these end-points to be established;

b) to have meaning to end-users to allow them to identify the source of an incoming communication (e.g. CLIP, email addresses) or to confirm identity of the remote end-point to whom a connection has or will be established (e.g. COLP, urls).

Failure to satisfy the first of these two functions may result in system failure and no service to end-users. To ensure such failures do not occur, very strict and rigid rules about the content and formatting of communication identifiers have to be enforced.

Most communications related identifiers to date have used either wholly numeric schemes (e.g. E.164 [9] telephone numbers) or alphanumeric schemes that are limited to the simple Latin alphabets (e.g. current e-mail addresses). With the increasing growth of the ICT markets in countries that use neither the simple Latin alphabet nor the same character sets, the ability to have a single communication identifier perform both of the above functions becomes increasingly difficult.

In UCI the two different functions above are performed by separate entities that have been chosen to perform their respective functions to the maximum effectiveness.

5.1.2 Identity and identifier hierarchy

An abstract model of identity and identifiers is given in figure 1. This considers two specialized forms of identity, authoritative and non-authoritative, with specializations of private, public and alias below.

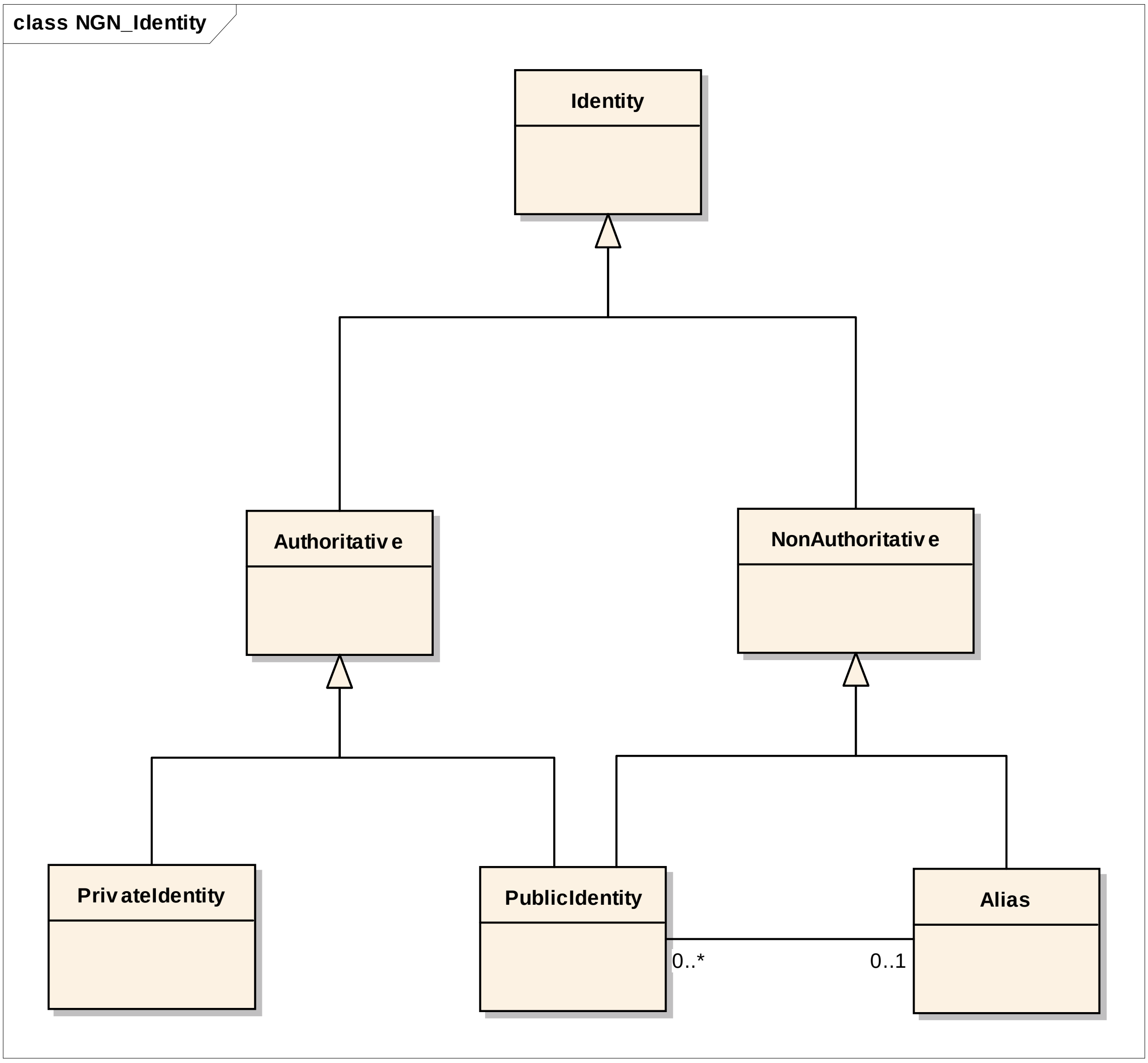


Figure 1: Abstract model of identity/identifier hierarchy

In UCI the structure is such that by allowing bindings of alias identity to an authoritative public identity the alias becomes authoritative by association.

In the context of figure 1 the UCI-numeric is an instance of a public-authoritative trusted identifier, UCI-label is an instance of a public alias identifier made authoritative by association to the UCI-numeric (which is authoritative).

5.1.3 UCI architecture

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).

NOTE: The service agent has also been referred to as a system agent in previous UCI documents but for the purposes of the NGN is referred to as a service agent as it acts to manage NGN services on behalf of the user (where the NGN is itself the system hosting the services).

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 services plane of NGN.

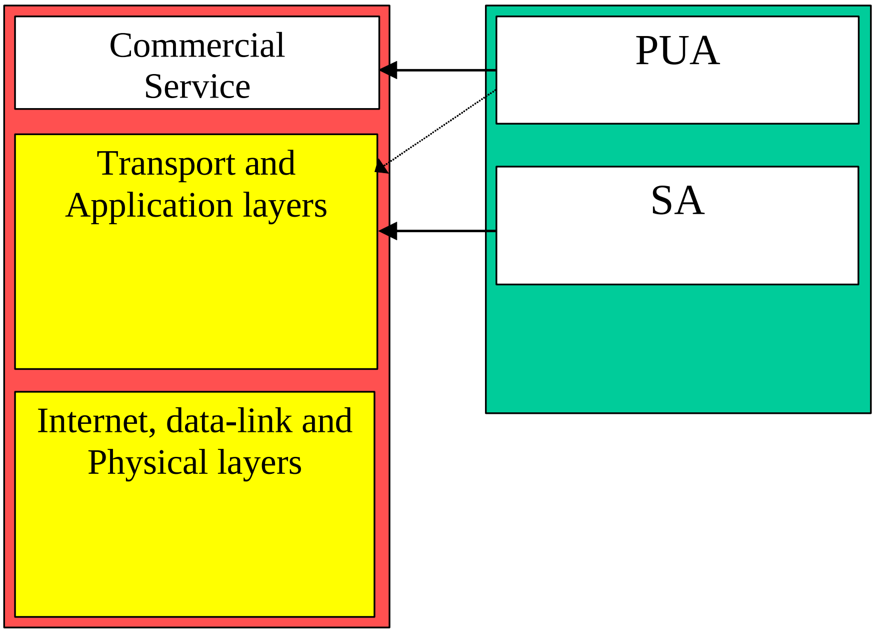
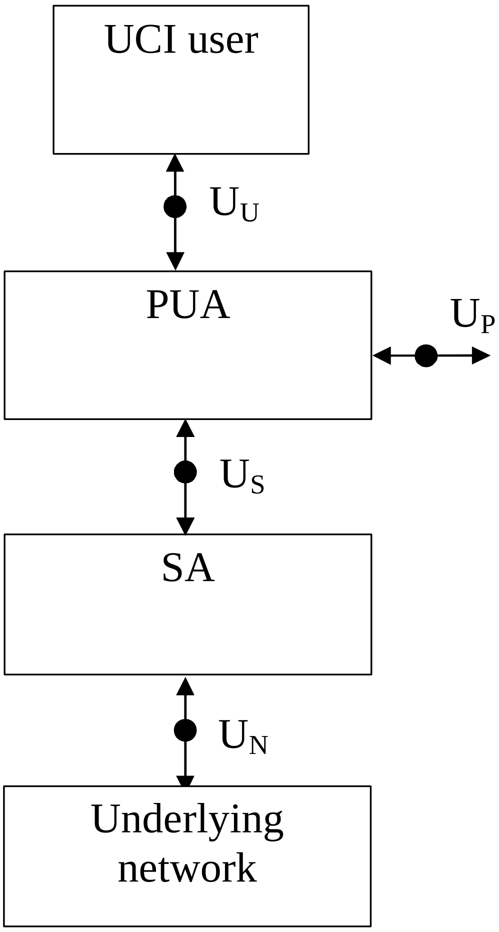

Commercial Service
Transport and Application layers
Internet, data-link and Physical layers
PUA
SA

Figure 2: UCI relationship with conventional (ISDN-era) protocol layering

In EG 203 072 [3] the interface between PUA and SA was described and recommended to be an open interface in order to allow adopters of UCI to feed the concepts into their networks or architectures.



A reference point between the PUA and the SA is defined as U_S.
A reference point allowing access to the PUA, and for communication between PUAs, is defined as U_P.
A reference point allowing the UCI user to access the PUA is defined as U_U.
A reference point allowing the SA to access the capabilities of the underlying network is defined as U_N.

Figure 3: UCI reference points

Terminals and end-user applications will vary, as will the access networks that connect these entities and the user's PUA. For this reason the technical solution for providing the required interconnectivity and interworking will vary according to the nature of the various entities.

EXAMPLE: An email application over an always-on broadband network may need a different solution to a PSTN telephone over a standard telephony network.

The data associated with UCI is not restricted to only the UCI but also includes a service profile maintained within the SA, and a user profile maintained within the PUA.

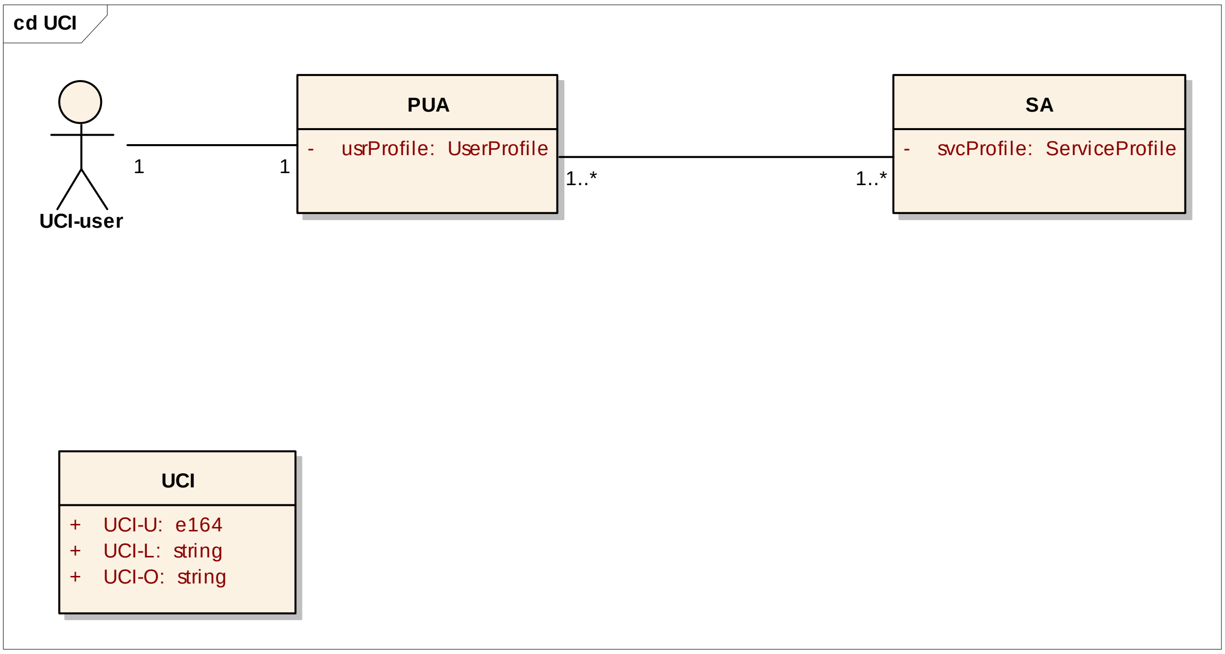


Figure 4: Cardinality of UCI relationships

5.1.4 UCI construction

The UCI has been specified in EG 203 072 [3] as a 3-part construct as follows:

- Numeric part:
  - This is unique across all UCI and has been designed to perform the function described in bullet point a) in clause 5.1.1.
- Label part:
  - Optional part that may be used to attach a user-name or other user-label to the numeric part of the UCI. The UCI may have zero, one or many labels. The label is provided exclusively to perform the function described in bullet point b) in clause 5.1.1.
- Additional data field:
  - The additional data field is optional and may be used to qualify the label (e.g. to indicate its authenticity or to indicate that the label is an alias).

A simple definition of UCI in XML is given as follows with a description of the definition given in table 3.

```
<!ELEMENT UCI (UCI-Numeric, UCI-Label*, UCI-AdditionalData*)>
```

Table 3: Description of UCI definition

child element	element declaration	meaning
UCI-numeric	(none)	Exactly one child element
UCI-label	*	Zero or more child elements
UCI-AdditionalData	*	Zero or more child elements

5.1.4.1 The UCI-numeric

The UCI-numeric is the information element that uniquely identifies the end-user, and which also identifies the end-user's PUA as a routable element. The UCI-numeric shall meet the following requirements:

- be resolvable to the uri of the PUA associated with the UCI (see clause 9);
- included in, or be identified as the source of, every PUA to PUA transaction;
- be deliverable to end-user terminals and applications to allow it to be stored in a terminal or application (c.f. ISDN CLIP);
- be suppressible and not delivered to end-user applications or terminals in certain classes of anonymous communication (c.f. ISDN CLIR).

The findings of EG 203 072 [3] recommended that the UCI-numeric structure follows that defined by E.164 [9] with the attendant administration of the number that this implies. However it is noted that the main requirements listed above can be met by an alphanumeric format with the exception, noted in the analysis of EG 203 072 [3], of being directly dialable from legacy PSTNs.

5.1.4.1.1 Stability requirement for the numeric element of the UCI

Many identifiers provided to service subscribers are only valid as long as the person using the identifier remains a customer of the service (e.g. the customer leases the right to use the supplied identifier). Currently, people who wish to contact another person use these service provider provided numbers to do so. These are, therefore, the identifiers stored in most people's address books. If the person being contacted has changed service providers, the stored identifier will no longer be valid and the person trying to reach them will fail to do so. This communication failure is made worse by the fact that calling users will typically have no means to identify the new identifier that should be used - therefore making the loss of contact permanent.

Telephone number portability was introduced to address the above scenario, but it is not universally available (e.g. portability between fixed and mobile numbering is not normally permitted) and there may be disincentives for users to request this portability if presented with attractive service offerings that require them to adopt a new identifier.

One of the most significant user requirements in the original work on UCI was that end-users should not be forced into changing their UCI (numeric) when they decide to change the providers of their communications and other services. This implies that it must be possible to guarantee that a UCI numeric can remain the same throughout the lifetime of the UCI user (which may be the lifetime of the individual who uses the UCI or may be the lifetime of the specified business role).

NOTE: Where the UCI numeric is covered by an E.164 numbering plan, some changes made to the numbering plan could contravene this requirement.

As well as benefiting end-users, UCI can also benefit the providers of telecommunications services. Because the service specific identifiers belonging to a UCI user are normally hidden from other end-users, UCI owning customers of telecommunications service providers will be less concerned if their service-specific identifiers are changed.

5.1.4.2 The UCI-label

5.1.4.2.1 Function of the UCI-label

With each UCI, a UCI user may associate a number of different labels.

Communication can be established by means of UCI without a label being used. For this reason, the UCI-label is defined as optional. However, the UCI-label is described in such a way that it brings unique benefits to end-users. For this reason, support for the handling of UCI-labels, at least in information exchanges between PUAs, should be a considered an essential (if not mandatory) part of any implementation of UCI.

The fundamental role of the UCI-label is to allow the UCI user to show a meaningful form of identification to the end-user at the other end of a communication. The three most common ways in which a UCI-label is expected to be used are:

- to present the UCI user's personal name (e.g. William Arthur Davies);
- to present some form of nickname instead of an officially recognized name (e.g. friendlybill);
- to present the name of the business role to which a UCI is assigned (e.g. ETSI Help desk).

The UCI-label is a separate entity to the UCI-numeric, although the relationship between these two entities is precise. The separation of these two entities enables them to perform their respective functions to the maximum effectiveness.

The XML description of the UCI-label is:

```
<?xml version="1.0" encoding="UTF-8"?>
<UCI-label>
  <type>Unstructured alphanumeric string</type>
  <!content>User-defined alphanumeric information</content>
  <characters>
    <minimum>0</minimum>
    <maximum>255</maximum>
  </characters>
  <character-encoding>UTF-8</character-encoding>
</UCI-label>
```

Previous UCI documents EG 201 940 [1], EG 202 067 [2] and EG 203 072 [3] identify three different label presentation options:

- authentic - this is the premium class of label and it indicates that a trusted third party has certified that the UCI user is entitled to call themselves by this label;
- alias - any label that is not authentic. It should be noted that this label may be a valid name for the UCI user, but it is identified as an alias as it has not been certified as authentic (almost all of today's identifiers for end-users fall into this category);
- anonymous - no label is presented (which should be distinguishable from failure to deliver a label).

The UCI-AdditionalData element (the third component of a UCI) data (see clause 5.1.4.3) is used to indicate to which of these three categories the label belongs. Putting "anonymous" in the appropriate child element of UCI-AdditionalData is the mechanism by which a true attempt to communicate anonymously can be distinguished from failure to deliver the label.

5.1.4.3 UCI-AdditionalData

As indicated in table 3, there may be zero or more child elements of UCI-AdditionalData. Previous UCI documents EG 201 940 [1], EG 202 067 [2], EG 203 072 [3] discuss many possible uses for UCI-AddionalData (referred to in these documents as "the additional information field"). The content of UCI-AddionalData is never intended to be presented to users. Child elements of UCI-AddionalData may, however, be processed by the PUA or the end-user's terminal or application to influence the way in which things are presented to the end-user (e.g. a UCI-AddionalData child element might trigger a change to some of the terminal's language settings).

The one child element that will have an effect on the use of, if not the design of, existing NGN functionality is the element that asserts that the label is either authentic, an alias, or anonymous. A PUA, on seeing this additional information, may initiate a process to validate the assertion - particularly for an assertion of authenticity of a label.

A proposed structure for this element is:

```
<?xml version="1.0" encoding="UTF-8"?>
<UCIAD-child name="Label_assert">
  <!purpose>To identify the existence and type of UCI-label in a UCI request or response</purpose>
  <type>binary</type>
  <numberofbits>2</numberofbits>
  <!bit-values>
    <!bit0 value="0">No label is present</bit0>
    <!bit0 value="1">A label is provided</bit0>
    <!bit1 value="0">The label is an alias</bit1>
    <!bit1 value="1">The label is calimed to be authentic</bit1>
  </bit-values>
</UCIAD-child>
```

Some of the broad, less well defined, categories in which this field may be used include:

- giving information on any special requirements that the user may have (e.g. as a result of a disability, or because they are driving a car, the user may request that all information is delivered in an audible form);
- providing a pointer to a sources of detailed specification of the user's language skills and preferences to be used to ensure that the best language variant of a service is delivered to that user;
- information intended for the initiator of the communication attempt that would accompany a rejection of the request giving details of alternative (perhaps non-electronic) ways in which the communication attempt could be pursued.

Ongoing ETSI activity on providing support related to language and disability related user profile information may help to clarify the requirements for UCI-AdditionalData content related to the first 2 items in the above list.

The information content related to the above and other uses of the UCI-AdditionalData may have little or no impact on any existing or planned NGN functions and protocols. The information that is conveyed would be processed by the Application Server functionality of the PUA and, thus, the rules for the interpretation and use of this information would be outside the scope of NGN standardization activity.

5.1.5 UCI Use Cases

The generalized UCI use case is shown in figure 5 showing the actors in UCI and the main activities that they perform.

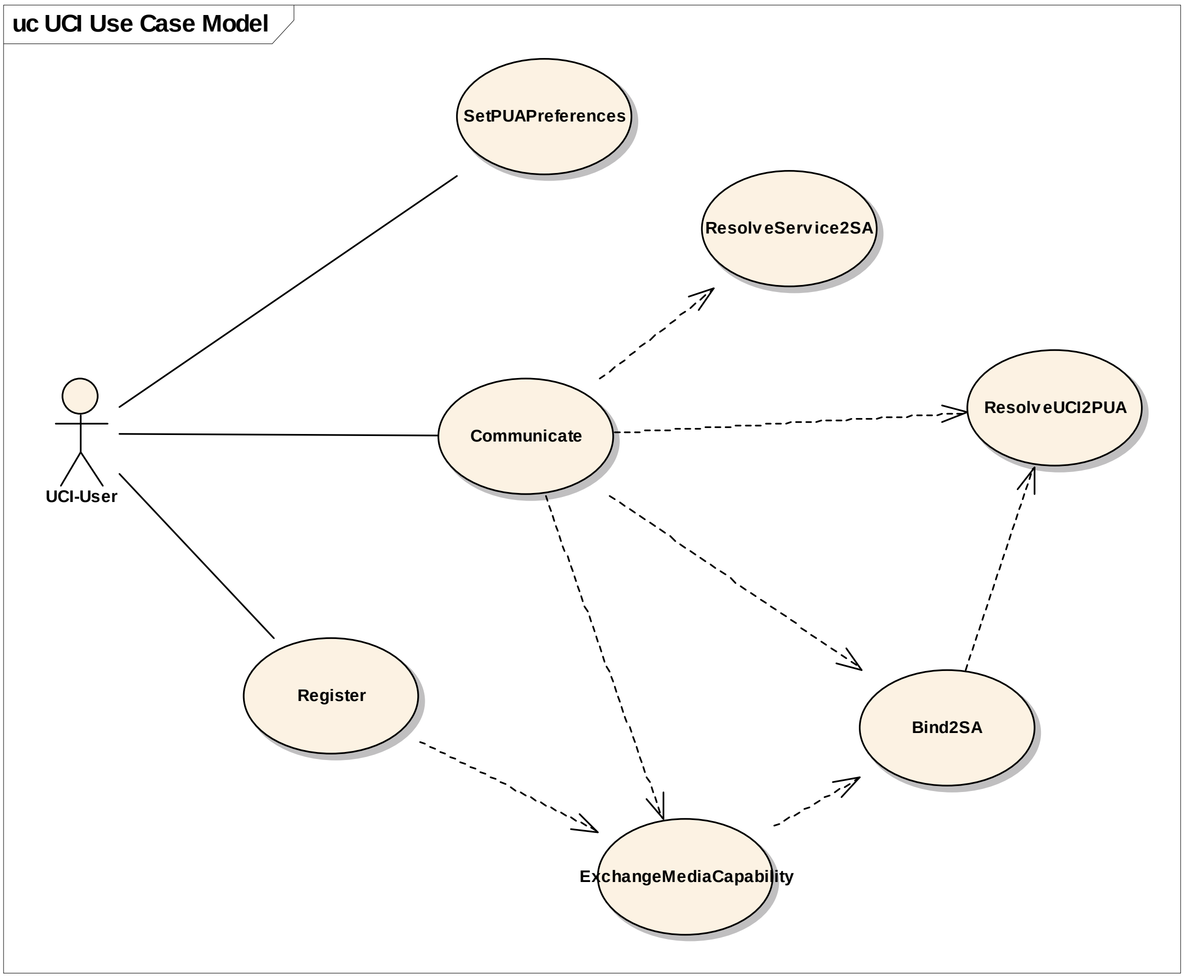


Figure 5: General UCI Use Case

5.1.5.1 Use case: register

This use case introduces the UCI-user as an actor. A UCI user wishes to activate his PUA to assign appropriate SAs for his subscribed to services at his current location. In order to do this the following data has to be exchanged by the user or on his behalf with the PUA:

- identity;
- set of services to be activated;
- terminal capability (i.e. what services the terminal is able to support);
- local network connection capability (i.e. what transport capabilities the local network is able to support (may be expressed in terms of bandwidth, symmetry, jitter, packet-loss, number of concurrent sessions, etc);
- location (network and if appropriate physical location of the user).

In response the PUA shall validate the user, the service set, the authority to invoke those services from the current location, the viability of offering each service in the light of the terminal and network capabilities. On success the PUA shall identify and assign an SA (or set of SAs) as appropriate.

5.1.5.2 Use case: Communicate

The "communicate" use case introduces a new actor to UCI, the "non-UCI user". The non-UCI user does not have access to all elements of the UCI.

In the case of a UCI user, a communication request and associated data is passed from the User to his PUA. The PUA interacts with the process rules use case to determine rules to be implemented during a communication set-up. Where the recipient is also a UCI user, a dialogue between the originating and recipient PUAs will occur.

In the case of a non-UCI user, no PUA exists. Communication policy is determined by the legacy manager by means of the process rules use case. In the case of PSTN user this is traditional telephony management.

The general UCI use case includes both UCI and non-UCI users for originating and receiving communications, thus enabling the set of communications instances described in table 4 to be constructed.

Table 4: Communications instances described by UCI

Instance	Originator	Recipient	Description
1	Non-UCI User	Non-UCI User	Legacy network e.g. PSTN (see note)
2	UCI User	Non-UCI User	Network directory/familiar names
3	Non-UCI User	UCI User	Limited call screening based on calling number
4	UCI User	UCI User	Full UCI capabilities supported
NOTE: This scenario does not invoke UCI capabilities and is not covered in the remainder of the present document.			

The establish communication process accepts communication requests from the User. The originator's PUA is responsible for determining the service type and routing (including, where appropriate, dialogue with the recipient's PUA) and for establishing communication through the Service Agent (SA).

5.1.5.2.1 Communication scenario 1: non-UCI user to non-UCI user

This scenario represents current telecommunications supported by today's networks e.g. PSTN, PLMN, IM/IP-services. Communication is established between the originating and terminating user without knowledge or use of UCI. The communication identifier is service specific. No use is made of UCI elements.

5.1.5.2.2 Communication scenario 2: non-UCI user to UCI user

This scenario considers where the recipient (the UCI user) is registered to receive services and can accept communications from a non-UCI user. As a minimum, the recipient's network needs to be capable of supporting UCI (e.g. the PUA for inbound service features). Limited use is made of the UCI capabilities (e.g. previously established processing rules may not be fully invoked).

Systems implementing UCI should interwork with legacy systems. The telephone networks at the location of the communication originator, and beyond, must be able to process the UCI-numeric and route a telephony call to a telephone belonging to the UCI owning recipient.

NOTE: This fits to the PES and PSS domains of the NGN.

A person wishing to contact a UCI user should be able to dial the numeric part of the UCI and make a voice telephony call to that person, the consequence of this requirement is that the numeric part of the UCI is in the same format as the legacy telephony networks, i.e. E.164 [9].

In considering legacy systems, and the evolution to an UCI type environment then greater granularity of assessment is required for that consideration.

5.1.5.2.3 Communication scenario 3: UCI user to non-UCI user

This scenario considers where the originator is registered to initiate UCI communications to other users. As a minimum, the originator's network needs to be capable of supporting UCI (e.g. the PUA determination of an SA for outbound service features). Limited use is made of the UCI capabilities (e.g. negotiation between PUAs to enhance the processing rules may not be fully invoked).

5.1.5.2.4 Communication scenario 4: UCI user to UCI user

This scenario considers where both the originator and recipient are UCI registered. PUAs and SAs exist to handle both outbound and inbound services. This includes negotiation between PUAs for the choice of communication. It is this ability for PUAs to negotiate that differentiates UCI communications from previous communications models (e.g. UPT). Full use is made of the UCI attributes to act on the rules contained within the PUAs to determine an optimum communication configuration.

A communication between UCI users, where PUA to PUA communication is used makes the requirement of the numeric element no more than an initial mechanism to establish the connection between PUAs. Once established, the negotiation phase begins and this uses data other than the numeric.

5.1.5.3 Use cases: Resolve UCI to PUA, Resolve Service to SA

The overall UCI Use case model shown in figure 5 identifies 2 resolution use cases and a binding use case. The resolution use cases are further shown as Message Sequence Charts in figures 7 and 8.

The resolution use-cases are shown in context of the UCI class diagram in figure 6.

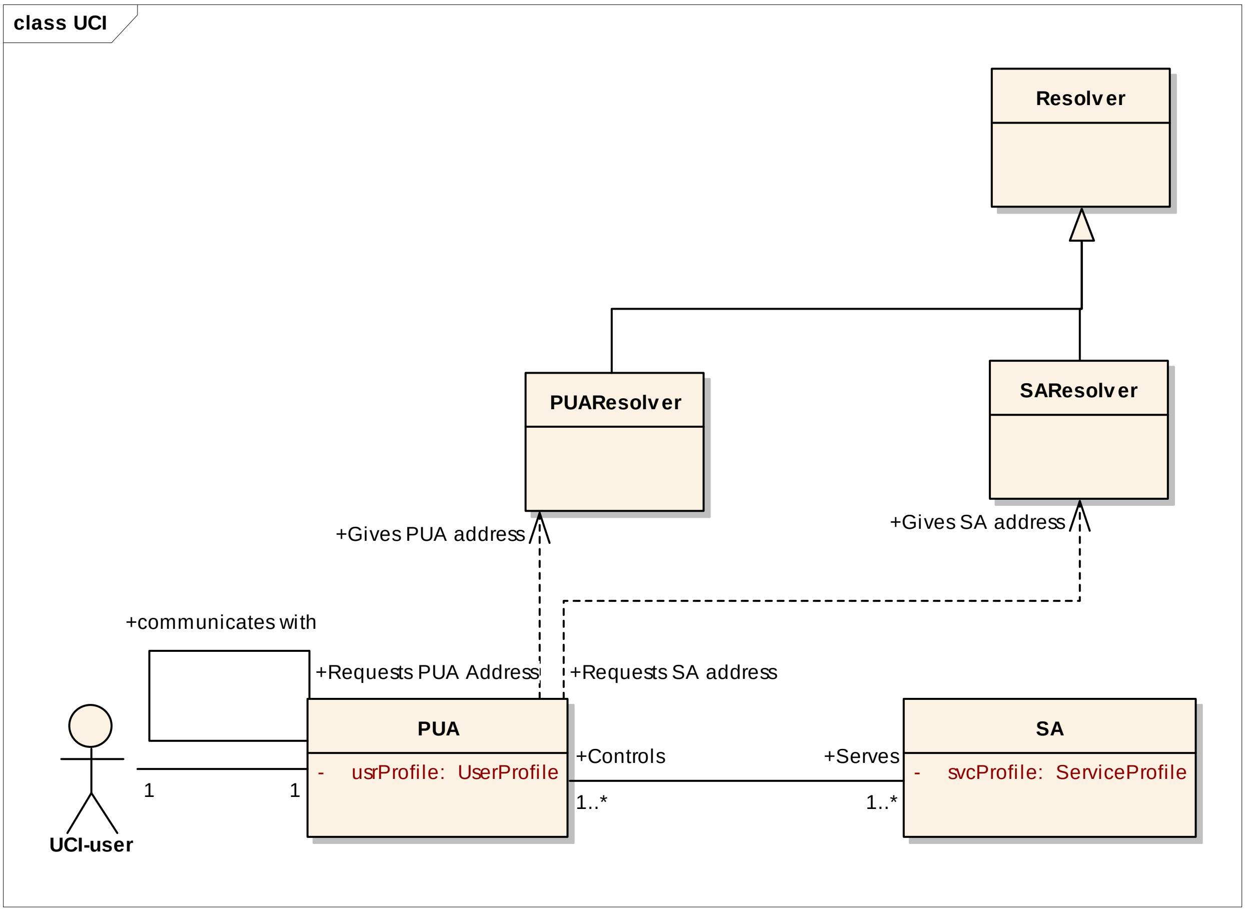


Figure 6: UCI class model highlighting resolver class relationships

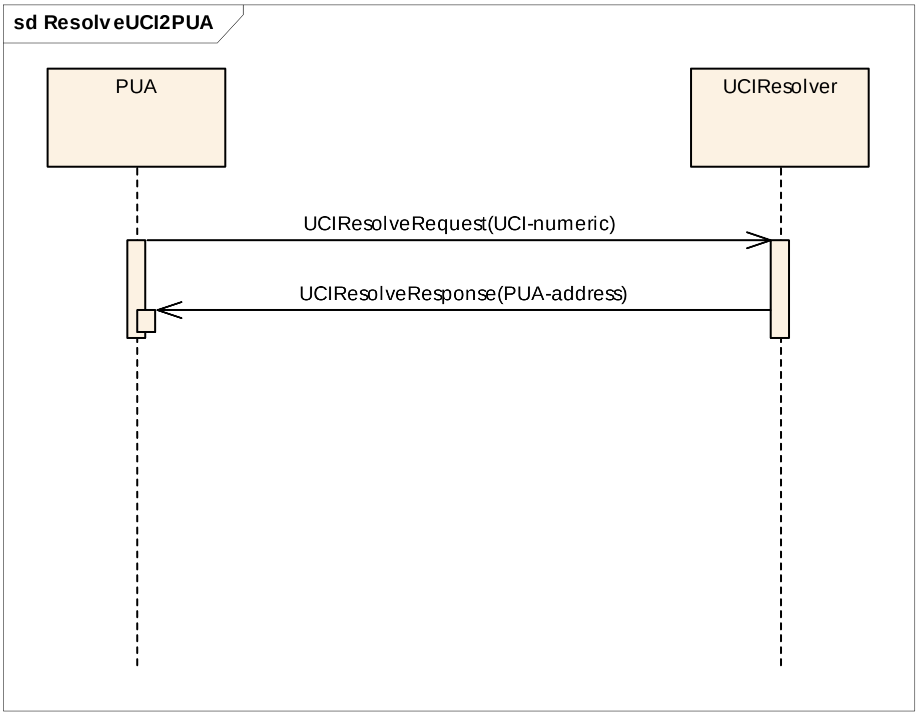

sd ResolveUCI2PUA
PUA
UCIResolver
UCIResolveRequest(UCI-numeric)
UCIResolveResponse(PUA-address)

Figure 7: UCI PUA resolution use case examination

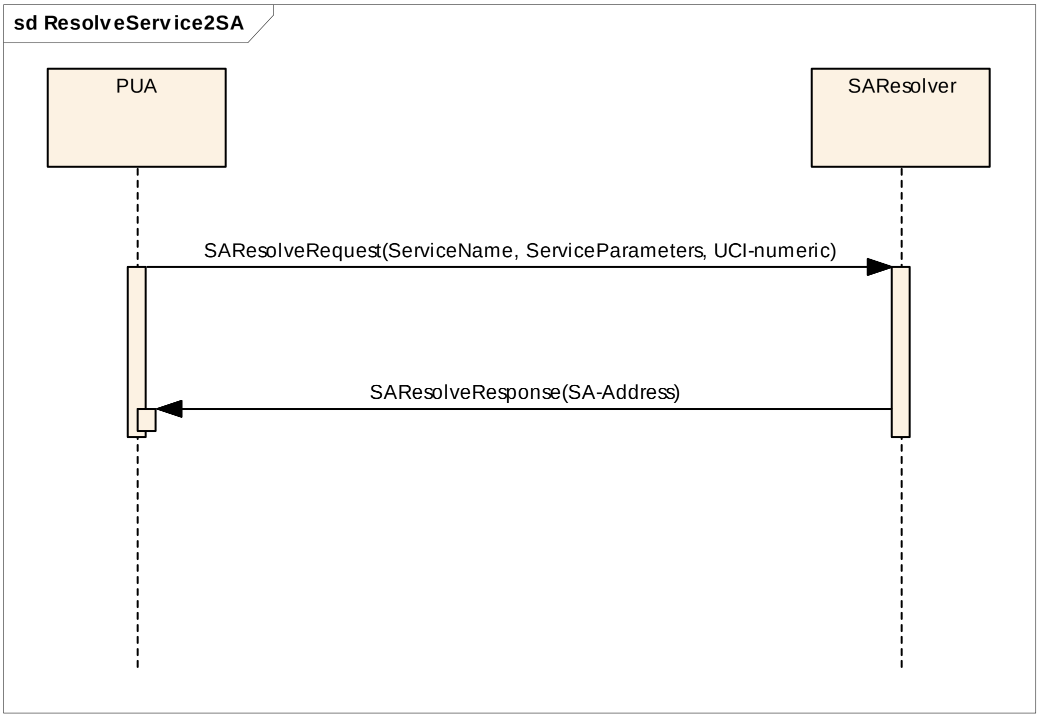

sd ResolveService2SA
PUA
SAResolver
SAResolveRequest(ServiceName, ServiceParameters, UCI-numeric)
SAResolveResponse(SA-Address)

Figure 8: UCI SA resolution use case examination

5.1.6 UCI related operational roles

To ensure that it was possible to examine different options for how UCI could be operated, a set of generic "roles" that relate to a significant function performed in the provision and operation of UCI were defined in clause 4.2 of EG 203 072 [3]. This approach meant that the operation of UCI could be thoroughly examined without making assumptions about what person or organization performs a specific role. Looking at different scenarios as to how UCI can be operated in practice then simply becomes a task of mapping these generic roles to specific people or organizations.

The table from clause 4.2 of EG 203 072 [3] is reproduced below to enable these same role names to be used in the context of the present document.

Table 5: Operational roles in UCI

Role	Description of function	New role for UCI (see note 1)
UCI Provider	Issues a user with a UCI (unique number and placeholder for label and "additional Information" fields)	√
Identity certification organization	Certifies that the user's chosen description in an "authentic label" is legitimate (see note 2)	√
Authentic-identity source	Acts as the authoritative source of valid personal identification data (e.g. name allocated at birth or legally changed name, date of birth and sex)	X
PUA Provider	Provides PUA service to the user	√
SA Provider	Provides SA services for a communications service provider (see also note 1)	√
Communications service supplier	Provides communications services to service subscribers (users)	X
Communications infrastructure provider	Provides the communications necessary to support a communications service (see note 3)	X
NOTE 1: Where a "New role" is identified this may be taken by an organization that already has an existing role in the telecommunications world or it may be taken by a "new entrant". Where a single organization wishes to take several roles, scrutiny by competition and regulatory authorities is likely. NOTE 2: Delegated From "Authentic identity source". NOTE 3: Where carrier selection is provided, users may wish to select their chosen carrier In this case it may be necessary to allow direct choice of carrier from a PUA. In this case SA functionality will need to be provided at the "communications infrastructure provider" layer.		

6 UCI incorporation to TISPAN NGN architecture

6.1 Overview of the UCI functional architecture

In the UCI system, every user role has an associated PUA, and every service has an associated SA. Where a user has a number of roles they may have a number of UCIs (e.g. a UCI for business use and another for personal use) and an equivalent number of PUAs as outlined in EG 202 067 [2].

NOTE: The use of multiple aliases may be used to associate multiple roles with a single UCI.

A PUA is a functional entity with a one-to-one relationship to a specific UCI. It stores or has access to information on all of a person's communication services and their service identifiers (e.g. telephone numbers, email addresses). The PUA also stores or has access to current status and personal preferences information in relation to these services (e.g. mobile phone switched on and reachable, not able to access home telephone, does not wish to receive emails at this time). A PUA participates in communication with its own user, other PUAs and SAs associated with the user's registration. It should never release personal information unless specifically authorized by the owner.

An SA is a functional entity that is linked to a communication service (or network). An SA is the link between the UCI and networks and services. It participates in communication with PUAs and its own network/service and would be specially trusted by PUAs following successful registration. The SA should never release personal information (such as dialable terminal identifiers) unless specifically authorized by the owner, but it can use this information to expedite the set-up of a communication.

The SA provides a consistent interface to the PUA irrespective of the internal architecture of its network/service.

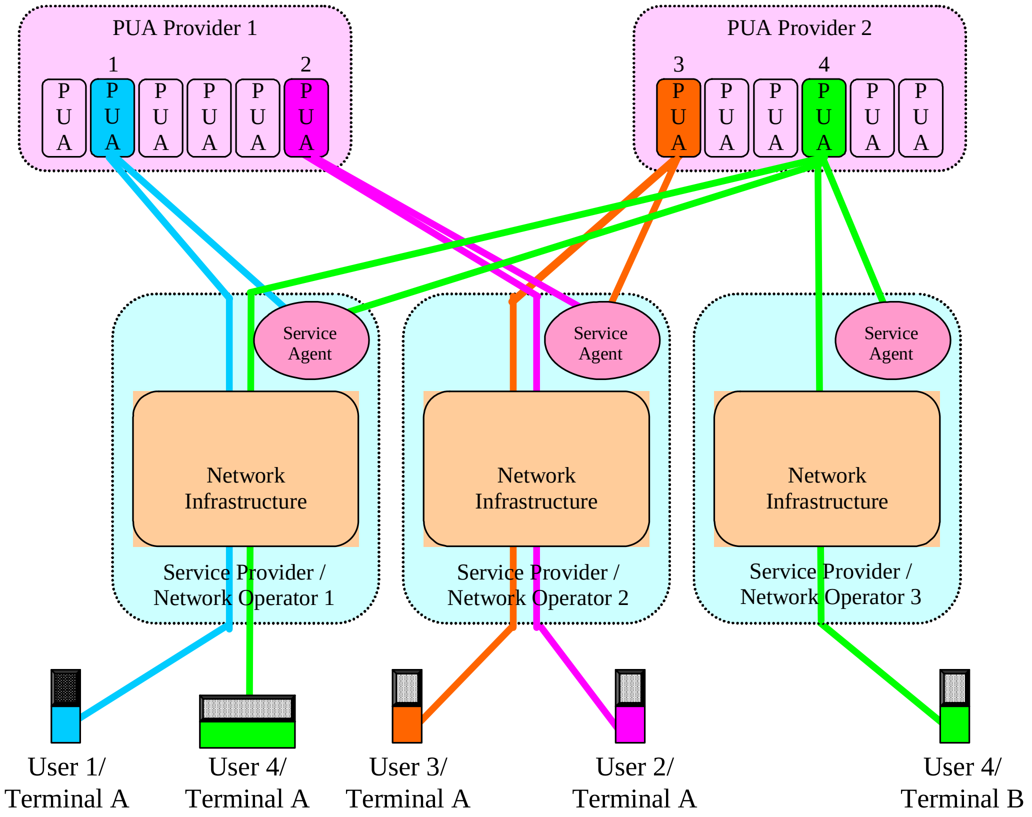


Figure 9: UCI Context Model

Figure 9 shows the physical relationship between PUAs, SAs, user roles and terminals. It shows how one user role can have a single PUA that helps the user to manage communication involving a number of terminals that are associated with a range of networks and services. It also shows how SAs are related to a communication service (or network) and that PUAs may be provided by a number of different PUA Provider organizations.

6.2 Mapping UCI and TISPAN NGN functional architectures

6.2.1 Personal User Agent

6.2.1.1 Functional decomposition of the PUA

To assist the mapping of the UCI and NGN functional architectures, a functional decomposition of the PUA has been introduced and is shown in figure 10 The functional entities have been chosen as those that would be needed to enable the PUA to perform all of the tasks that are stated or implied in the wide range of requirements and scenarios documented in the previous UCI documents EG 201 940 [1], EG 202 067 [2] and EG 203 072 [3].

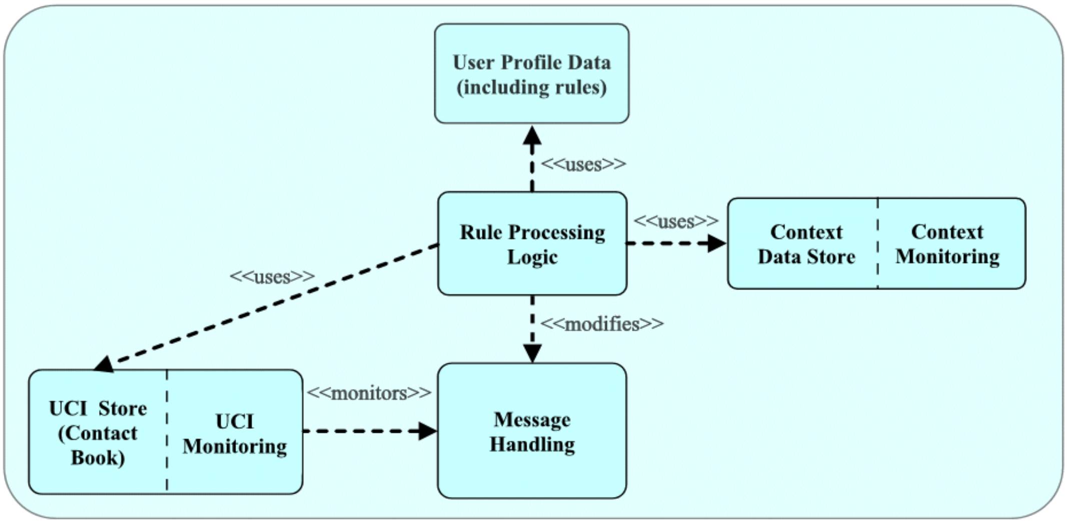


Figure 10: PUA logical functional entities

In the following clauses, the functional entities shown in figure 10 are referred to with surrounding quotation marks e.g. "Message Handling".

6.2.1.2 Use case: Register

The following actions are undertaken by the PUA in the course of registration:

- Validation of the user identity (PUA stores in the "UCI Store (Contact Book)" or has access to information on all of a person's communication services and their service identifiers (e.g. telephone numbers, email addresses, etc.).
- Validation of the user location (network and if appropriate physical location of the user).
- Validation of a set of services to be activated.
- Validation of the authority to invoke the services from the current location.
- Validation of the viability of each service in the light of:
  - terminal capability;
  - local network connection capabilities.
- Identification and assignment of an SA (or set of SAs) as appropriate.

NOTE: The identification and assignment of an SA is described by use cases ResolveService2SA and BindSA.

- Storage and access to current status (in the "Context Data Store") and personal preferences information in relation to these services in "User Profile data (including rules)" (e.g. mobile phone switched on and reachable, not able to access home telephone, does not wish to receive emails at this time, etc.).

In a use case "UCI Registration" for the NGN defined by TISPAN the User Profile Server Function (UPSF) defined by TISPAN NGN in ES 282 001 [20] maps to the functionality of the PUA through its ability to store data related to the following:

- Service-level user identification, numbering and addressing information.
- Service-level user security information: access control information for authentication and authorization.
- Service-level user location information at inter-system level: the UPSF supports the user registration, and stores inter-system location information, etc.
- Service-level user profile information.

The source of the context data in the "Context Data Store" is "Context Monitoring" which maps to the NGN presence Server.

It should be noted that the data stores described above may be realized as a set of federated sources. This is an approach taken by the Liberty Alliance Project Identity Federation Framework (ID-FF) as identified in annex C.

6.2.1.3 Use case: Process rules

The following actions are undertaken by the PUA in the course of Process rules:

- Introduction of the "Legacy manager" to UCI (The legacy manager represents the management of a network/service that has been upgraded to interwork with, or to comply with, UCI).

In a use case "Process rules", the Application Server (AS) defined by TISPAN NGN maps to the functionality of the "Rule Processing Logic" component of the PUA through its ability to process data, i.e. its ability to provide standalone services or value added services on top of a basic session. An example is when a Public Service Identifier is hosted by an Application Server and the Interrogating-CSCF forwards SIP requests destined to a Public Service Identifier directly to the Application Server as specified in [7].

6.2.1.4 Use case: Communicate

The PUA establishes the parameters to be used in establishing the session and therefore drives the session establishment. Based on the "Process Rulers", the PUA handles the messages for the communication which is a task which corresponds to the session control for the establishment and management of SIP based communication sessions provided by the Call Session Control Function (CSCF) in TISPAN NGN. Therefore, the Call Session Control Function (CSCF) defined by TISPAN NGN maps to the functionality of the "Message Handling" component of the PUA in the use case "Communication".

6.2.1.5 All use cases

Those elements of the functional decomposition of the PUA that are referred to in the analysis of the individual use cases for which no explicit mapping has been identified all map to sub-functions of the AS that was identified in the analysis of the "Process Rules" use case.

6.2.2 Service Agent

In the UCI model the following actions are undertaken by the SA:

- participation in communication with PUAs and a particular network or service (potentially one SA per network type or service type);

- interpreting the standardized session control protocols from a PUA into an appropriate form for the control mechanisms provided by the network or service with which the SA is associated;

- set-up of a communication session by using the session control protocol appropriate for the controlled network or service.

As already stated in the previous section, in a TISPAN NGN, the Call Session Control Function (CSCF) performs the session control for the establishment and management of SIP based communication sessions. Therefore, as the CSCF is mapped as a component of a PUA, its session control protocols need no interpreting and therefore no SA is needed.

In setting up a connection with a PSTN/ISDN network that uses the ISUP protocol, the SIP protocol from the PUA needs to be mapped to the ISUP protocol. In NGN, Signalling Gateway Function (SGF)and Media Gateway Control Function (MGCF) already performs the necessary protocol mapping, therefore the SGF and MGCF can be said to be the SA for controlling ISUP based PSTN/ISDN networks.

If it is required to establish a session with other IP network or service, then the SIP request is forwarded to Interconnect Border Control Function (IBCF) which serves as the entry point to the other domain. The IBCF can insert the Interworking Function (IWF) in the signalling route when appropriate. Thus, IBCF and IWF can be said to be SA for controlling other IP networks.

6.3 Mapping UCI and NGN functional entities and reference points

The analysis of the use cases in clause 6.2 has led to the mapping of the UCI functional entities to NGN functional entities shown in table 6. The entities derived from the functional decomposition of the PUA are referred to by the names assigned to them in figure 10.

Table 6: Mapping UCI and NGN functional entities

UCI functional entity	PUA decomposition entities	NGN functional entity	Notes
PUA	User Profile Data (including rules)	UPSF	
	Content Monitoring	NGN Presence Server	
	Rule Processing Logic + UCI Store (Contact Book) + UCI Monitoring + Content Data Store	AS	
	Message Handling	CSCF	The CSCF can act as Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF) or Interrogating CSCF (I-CSCF).
SA	-	MGCF, SGF (BGCF, MGCF, SG)	For IMS to PSTN/ISDN connection. The functional entities in the brackets apply if Breakout Gateway Control Function (BGCF) is involved in the session. The involvement of BGCF to the session depends on the transit scenario supported by IMS.
NOTE: Where border control functions (e.g. IBCF) are used, PUAs will communicate with each other via these border control functions. There is nothing inherent in using these border control functions that should impact on the UCI use cases in any way. Where border controls are used, it is no longer possible to identify a single NGN functional entity, but logically the two PUAs still communicate directly with each other.			

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 table 7.

Table 7: PUA placement impact on NGN

Scenario	PUA placement	Notes
A	Outside the NGN	Requires a new interface between PUA and NGN.
B	Inside the NGN as new component	Requires definition of new internal reference points between PUA and NGN functional entities.
C	Inside the NGN using existing components	The mappings defined in the remainder of the present clause apply.

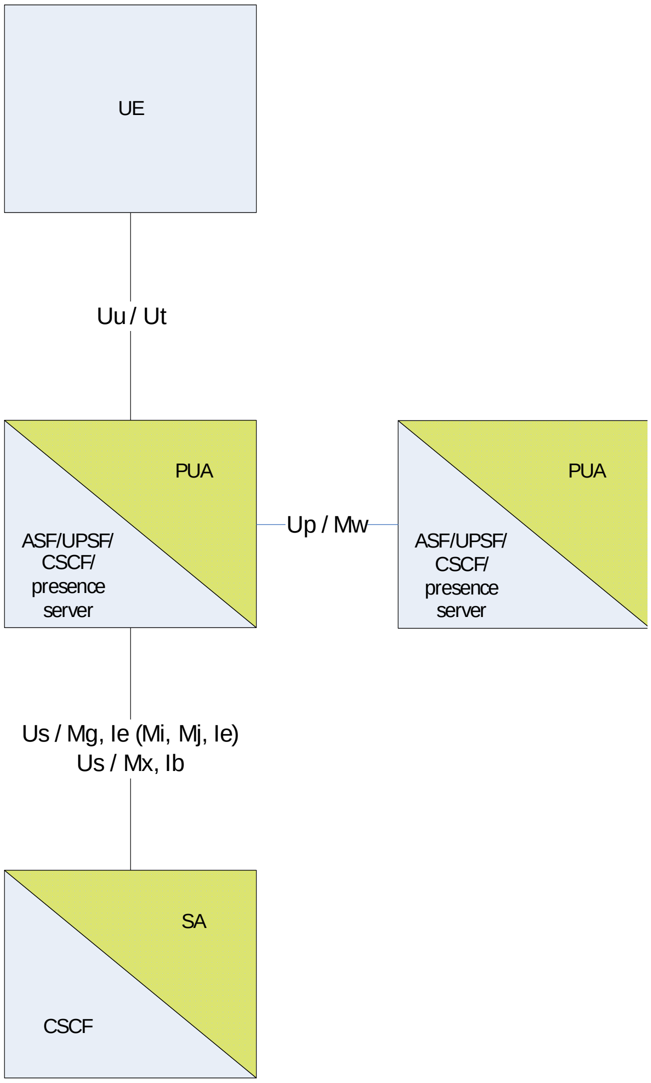
Table 8: Mapping UCI and NGN reference points

Use case	UCI reference point	NGN reference point	Notes
PUA: UCI registration	Us	Cx	For NGN to NGN connection (see note).
PUA: Process Rules	Us	ISC	
PUA: Communicate	Up	IMw	
SA	Us	Mg, Ie (Mi, Mj, Ie)	For NGN to PSTN/ISDN. The reference points in the brackets apply if Border Gateway Control Function (BGCF) is involved in the session. The involvement of BGCF to the session depends on the transit scenario supported by IMS.
SA	Us	Mx, Ib	For IMS to other IP networks, or between two IMS networks, if border functions are applied.
NOTE: Where border control functions (e.g. IBCF) are used, PUAs will communicate with each other via these border control functions. There is nothing inherent in using these border control functions that should impact on the UCI use cases in any way. Where border controls are used, it is no longer possible to identify a single NGN reference point, but logically the two PUAs still communicate directly with each other.			

6.4 Summary

The mapping of PUA to a combination of UPSF, ASF, CSCF and presence server is clearly identified. The mappings of the reference points Us to a combination of Cx and ISC, of Up to Mw and of Uu to Ut is also clearly identified for the connection within IMS, or if no border control functions are applied.

The mapping of SA is more complex than for PUA, as the form of the SA will change according to the type of communication session being established. It has been identified that no SA is required for NGN SIP communication sessions within the same IMS network, or between two IMS networks, if border control functions are applied. For establishing sessions to PSTN/ISDN networks, the Signalling Gateway Function (SGF) and Media Gateway Control Function (MGCF) can be mapped to the SA. For establishing sessions with other IP network or service, or between two IMS networks, when border functions apply, the Intermediate Breakout Control Function (IBCF) and the Interworking Function (IWF) may be mapped to the SA. The reference point Us can be then mapped to the Mg, Ie (Mi, Mj, Ie) reference points for the NGN to PSTN/ISDN connection and to Mx, Ib reference points for the NGN to other IP network or between two IMS networks, if border functions apply, is identified, too. The preceding analysis is summarized diagrammatically in figure 11.



NOTE 1: Entities in blue colour are from the NGN.
NOTE 2: Entities in sand colour are from UCI.
NOTE 3: Interfaces are shown as UCI/NGN.

Figure 11: UCI mapping to NGN entities

7 UCI incorporation to TISPAN NGN protocol suite

7.1 Handling of the UCI in communication sessions

7.1.1 Generic issues related to the handling of a UCI

The 3 UCI elements are:

- UCI-numeric (the numeric element);
- UCI-label (the alphanumeric label);
- UCI-AdditionalData (the additional information field).

In the following clauses, the way in which these need to be handled by networks, services, applications and end-users is described.

Existing UCI documents ([2], [3]) give the responsibility for delivering all or part of the UCI to the end-user to the PUA that belongs to the end-user who receives the UCI. This contrasts with conventional telephony scenarios where the delivery of CLI information is initiated at the distant end of a communication. A more detailed rationale for why this model has been chosen is given in clause D.2, but in summary it is because:

- existing methods of delivering information that describes the identity of the originator of a communication, from the remote end, are all subject to active misuse that is designed to falsify this information;
- a UCI user's PUA will have received presence information about the UCI user and their associated services, terminals and networks that can assist it in determining the best way to deliver the information;
- a principal role of the PUA is to protect and manage identity issues on behalf of its own user.

Because the PUA knows the status of and has signalling and control access to all of the UCI user's terminals and services, it is not constrained to deliver the remote party's UCI-label using the same service or terminal that will be used for the proposed communication session. However, in the absence of other constraints, it should be to the benefit of both the end-user and the service provider, that delivery to the target terminal using the planned service will be the first option investigated.

Whereas this approach may sound more complex than the simple but imperfect solutions currently used, a number of new benefits can be offered to end-users. Some examples include:

- delivery of a spoken version of the caller's name to a phone that has a display - which would be relevant for both car drivers and blind users;
- delivery of a spoken version of a label to a telephone that has no display;
- use of an SMS to a mobile phone or an instant message to a PDA to display the name of the caller when the simple PSTN telephone is unable to display the Kanji characters used by the caller.

These examples show that examination of terminal capabilities, although an advance on trying to display a message that does not match those capabilities, may not yield a UCI-label display strategy that meets the user's requirements. In summary, the strategy on how to deliver the UCI-label information to a UCI user can and should take account of at least the following information:

- the end-users preference at the current time and place;
- the capabilities of the target device for the proposed communication to display the label data;
- the capabilities of the target service to deliver the label data;
- the range of terminals and services that can currently be used to best meet the end-user's requirements.

Whilst this might sound ambitious, today similar cross-service delivery mechanisms are increasingly being used. For example, SMS and voicemail are often used to deliver user identification related information about incoming emails to end-users.

There also needs to be a close tracking and alignment between the New Work Item on "Requirements for multimedia identity presentation" and the UCI identification presentation issues described in clause 7.1.1, as UCI could use any core NGN identification presentation service if the specification of that service met the needs of UCI presentation. Failure to assure alignment would lead to the need for an alternative identification presentation service to meet the needs of UCI or future changes to the NGN identification presentation service to meet those needs.

7.1.1.1 Delivery of the UCI-label

UCI specifications require that a UCI-label is delivered to each party in a communication independent of what communication mechanism is being used. As a minimum, UCI-labels will be stored in a user's PUA as a UTF-8 string.

The core UCI-related transaction in which the UCI-label will be communicated is in the exchange of information between PUAs. The form of data interchange chosen for this transaction should be capable of supporting all UCI-labels irrespective of their length.

When the information in the UCI-label is presented to an end-user, several factors related to the length and content of the UCI-label emerge. These include:

- the capabilities of the transport mechanism between a PUA and an end-user terminal;
- the transport of the UCI-label between a PUA and a non-UCI user;
- situations where a PUA is unable to deliver the UCI-label to its own user;
- the modality (e.g. text, speech) in which the end-user requires the information contained in the UCI-label;
- the capabilities of the terminal that presents (visually or audibly) information from the UCI-label to the end-user.

Each of these factors will be addressed separately in the following clauses.

The benefits of the UCI concept of having a single identifier (or very restricted number of them), that works for all services, and that is associated with sophisticated control mechanisms is described in clause D.3. This major UCI benefit will be undermined each time a user's service related identifiers are made public. For this reason, a major aim when implementing UCI should be to suppress the delivery of information that reveals these service specific identifiers (e.g. telephone numbers, email addresses). This leads to the following generic approaches:

- use existing methods of delivering user identification information and substitute UCI information for information that can reveal a user's service specific identifier;
- use existing methods to suppress the delivery of a user's service specific identifier (for telephony this could be by using CLIR which would have the effect of suppressing both the calling line and calling name identification information) and then use an additional mechanism to deliver the user's UCI identification information. The NGN TIR [8] simulation service does not yet guarantee that link to suppress Calling Name as there is yet no TISPAN Calling Name service specification.
- as there is a WI in TISPAN for a new Name Presentation service, there is an excellent opportunity to ensure that this service can be used in a UCI context according to the first of the above approaches.

NOTE: PSTN telephony fields for transmission of name information are based on 7-bit coding that is inadequate to meet the needs of transferring adequate naming information in a global multicultural environment. For this purpose, only UTF-8 [23] or better mechanisms will be required.

8 UCI incorporation to TISPAN NGN NNA suite

8.1 Numbering

The UCI-numeric is composed of an E.164 [9] compliant part and therefore complies with the E.164 regime of the NGN defined in TS 184 002 [21].

The use of labels in UCI does not have to be strictly controlled and collisions are allowed as only the UCI-numeric has a role in communication setup. Labels, and additional UCI information, only have relevance at the end-points of communication and in the delivery of information to the end-user and as such do not form part of the TISPAN NGN NNA suite.

8.1.1 Use of ENUM/DNS in UCI

ENUM or DNS may be used to implement the UCI to PUA resolution service. In such cases ENUM/DNS may be considered as instances of the "Resolver" class as shown in figure 12.

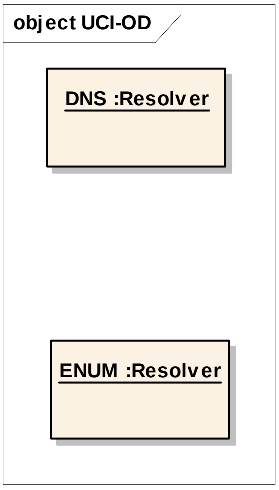


Figure 12: DNS and ENUM as instances of Resolver class

Where ENUM is used as a TISPAN number resolution service, the UCI numeric can be placed as a single entry in a NAPTR record. This entry would contain the URI of the user's PUA and specify the service type as "uci".

EXAMPLE: $ORIGIN 6.6.7.3.6.0.4.8.8.7.4.4.e164.arpa. IN NAPTR 102 10 "u" "uci+E2U" "!^.*$!uci:447884063766@puaprov1.net!"

In order to ensure that session establishment to UCI users can be guaranteed from the very earliest phases of the introduction of UCI, it is advised that an additional entry is placed in the NAPTR record using the SIP URI scheme. Apart from the scheme identifier, the content of the URI can be identical to that of the entry using the UCI URI scheme. This ensures that those ENUM clients and SIP clients that are unaware of UCI will be able to successfully establish SIP sessions with a UCI user.

9 Security analysis of UCI in NGN

9.1 Overview of assets, vulnerabilities and risk

The primary assets in UCI are as follows:

- UCI-numeric
- PUA identity
- PUA location
- SA identity
- SA location
- Interfaces that implement the UCI reference points
- Protocols that implement the UCI capability suite

Of these assets the NGN modelling and implementation described for UCI in the remainder of the present document is to use SIP, SDP and ENUM each of which has been analysed in TR 187 002 [16]. The analysis from TR 187 002 [16] applies to UCI.

9.2 Objectives

The security of UCI when deployed requires prevention of masquerade (i.e. to be able to assure other users that the identity of the claimant is that of the claimant). In order to give some of this assurance the communication from the UCI-user to the PUA across reference point U_U should be protected from eavesdropping and from malicious modification.

9.3 Review of security requirements from TS 187 001 v1.1.1

The requirements given in table 9, taken from TS 187 001 [4], apply to UCI. Where no comment is given the requirement applies without change to UCI in the NGN.

Table 9: Requirements from TS 187 001 [4] as they apply to UCI

Requirement-ID	Requirement text	Notes applicable to UCI
(R-SP- 3)	The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.	
(R-AA- 1)	Access to NGN networks, services, and applications shall be provided for authorized users only.	UCI requires that an authentic identity is presented and validated.
(R-AA- 15)	Mutual authentication shall be supported between the UE and the AS before providing authorization.	
(R-AA- 23)	The attributes required for authentication of a user by the access network maybe provided by the network operator to whom the user has a NGN IMS subscription.	When UCI is overlaid on IMS there may be some characteristics of the UCI defined by the operator.
(R-IR- 2)	An access identity shall be used for access authentication. This identity may or may not be used for other purposes.	
(R-CD- 10)	It shall be possible to protect sensitive data (such as Presence information and notifications) from attacks (e.g. eavesdropping, tampering, and replay attacks).	
(R-CD- 13)	Integrity protection of signalling, control communications and of stored data shall be provided.	
(R-CD- 14)	It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.	
(R-CD- 17)	Data integrity shall be supported between the UE and the Application Server.	
(R-CD- 18)	Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.	
(R-CD- 19)	Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.	
(R-CD- 22)	It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.	

Requirement-ID	Requirement text	Notes applicable to UCI
(R-P- 2)	User location and usage patterns shall be kept from unwanted disclosure.	
(R-P- 3)	It shall be possible to protect the confidentiality of user identity data.	Defined within use case "Set PUA preferences".
(R-P- 4)	Anonymous communication sessions shall be supported in NGN either in a permanent mode or in a temporary mode communication by call. In this case the originating party identity shall not be presented to the destination party. The network to which the destination party is connected to is responsible to handle this service.	Defined within use case "Set PUA preferences".
(R-P- 5)	NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.	Defined within use case "Set PUA preferences".
(R-P- 7)	The NGN shall support mechanisms for the network operator to guarantee the authenticity of a user identity presented for an incoming call to a user where the call is wholly within that operator's network (i.e. originating and terminating parties are subscribers to, and resident in, a single NGN).	
(R-P- 8)	The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.	
(R-P- 9)	The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentity).	Defined within use case "Set PUA preferences".
(R-P- 10)	A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided.	Defined within use case "Set PUA preferences".
(R-P- 11)	Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.	Defined within use case "Set PUA preferences".
(R-P- 12)	It shall be possible for the sender of the message to request to hide its public ID from the recipient.	Defined within use case "Set PUA preferences".
(R-P- 13)	Users may select the Identity information presented when starting a session or sending a message. It shall be possible to verify this identity information and to initiate a session or message in reply.	Defined within use case "Set PUA preferences".
(R-AD- 1)	Mechanisms shall be provided to mitigate denial-of-service attacks.	

10 Regulatory aspects as they apply to UCI

NOTE: If E.164 is used for the UCI-numeric then the existing regulatory schemes apply.

10.1 Access Directive

The Access Directive, 2002/19/EC [10] is intended to harmonize the regulation of access and interconnection of ECNs. The directive achieves this by establishing a set of obligations on CSPs who seek access or interconnection.

NOTE: Access in the directive does not refer to access by end-users.

In the context of UCI the provisions of the access directive do not address identity and therefore it can be concluded that UCI is not directly affected by the Access Directive.

10.2 Authorization Directive

The Authorization Directive, 2002/20/EC [11] identifies an obligation under article 5 for the rights of use of numbers and these are clarified in annex C of the Directive under which obligations can be placed on the CSP on the use of numbers. In particular the provision of number-portability and directory information are cited as conditions that may be attached to a number assignment.

The use of UCI, in particular the requirement that UCI "belongs" to the individual, enforces some form of number portability that has to be supported by the CSP.

10.3 Directive on privacy and electronic communications

The content of the Privacy Directive 2002/58/EC [14] applies to all CSPs and does not impose any additional constraints as a result of using UCI.

10.4 Universal Service Directive

10.4.1 Number portability

The use of UCI, in particular the requirement that UCI "belongs" to the individual, enforces some form of number portability that has to be supported by the CSP.

10.4.2 Directory Enquiry

Directory enquiry services are required under the provisions of the Framework Directive [12] and The Universal Service Directive (2002/22/EC [13]) in Article 25 states:

1) Member States shall ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a).

2) Member States shall ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory.

3) Member States shall ensure that all end-users provided with a connection to the public telephone network can access operator assistance services and directory enquiry services in accordance with Article 5(1)(b).

4) Member States shall not maintain any regulatory restrictions which prevent end-users in one Member State from accessing directly the directory enquiry service in another Member State.

5) Paragraphs 1, 2, 3 and 4 apply subject to the requirements of Community legislation on the protection of personal data and privacy and, in particular, Article 11 of Directive 97/66/EC [23]."

11 Recommendations for TISPAN NGN

11.1 UCI in the context of other developing standards work

The primary suite of standards required for the provision of UCI is the suite of NGN specifications.

In addition the work of the Liberty Alliance in the context of NGN is described in annex C. Complimentary work in the area of user profile management is being undertaken in ETSI Technical Committee Human Factors (TC HF) and this is being pursued for implementation in both TISPAN and 3GPP.

11.2 Recommendations

11.2.1 UCI NAPTR record type

As the proposed operation of UCI within an NGN uses SIP, the URI form of a UCI can be expressed as a SIP URI. However, this relies on examination of SIP INVITEs and RESPONSEs to discover that the originator of the INVITE and/or the responder are UCI users. Relying on this discovery may inhibit some UCI behaviours and may introduce both inefficiency and session setup delay. If however the ENUM NAPTR record of a UCI user has an entry that uses the "uci" URI scheme, the existence of a UCI capability becomes immediately apparent and this fact can be exploited from the beginning of the SIP session. For this reason, a new URI scheme "uci" should be developed within TISPAN and the IETF, for registration with IANA. UCI can be enabled in the NGN without change to any existing protocols. However to support UCI the existing profiles of existing protocols, in particular SIP and SDP, should be extended to allow UCI as a replacement of the existing SIP-url.

11.2.2 User = UCI

As an alternative to the development of a new URI scheme for "uci" it may be sufficient to have a "user=uci" parameter in the SIP-uri instead of the "user=phone" parameter.

11.2.3 Format of UCI-numeric

The form, and format, of the UCI-numeric element has to be structured as unique in the international context of the UCI in NGN.

11.2.4 Optimization of AS function for UCI

There is a requirement to specialize the Application Server to provide PUA/UCI capabilities. Ideally this should be referred to as PUA-AS but may also be considered as UCI-AS. The function of the PUA-AS is to perform those functions of PUA not already covered by straightforward profiling of ENUM, SIP and SDP (see clause 4).

11.2.5 SIP best practice

PUA initiated communication sessions should follow the "best current practices" documented in RFC 3725.

Annex A (normative): Mapping of UCI to Session Initiation Protocol (SIP)

A.1 Overview

The Session Initiation Protocol (SIP) is defined in RFC 3261 [5] and has been developed within 3GPP as the core signalling protocol for IMS. As defined in RFC 3261 [5] SIP supports five facets of establishing and terminating multimedia communications:

- **User location:** determination of the end system to be used for communication;
- **User availability:** determination of the willingness of the called party to engage in communications;
- **User capabilities:** determination of the media and media parameters to be used;
- **Session setup:** "ringing", establishment of session parameters at both called and calling party;
- **Session management:** including transfer and termination of sessions, modifying session parameters, and invoking services.

SIP is not a vertically integrated communications system. SIP is rather a component that can be used with other protocols to build a complete multimedia architecture. The Session Description Protocol (SDP) defined in RFC 2327 [22] is used for describing multimedia sessions.

The main architecture of SIP, with UCI mapped to it is shown in figure A.1, the special case of the NGN Back-to-back user agent is shown in figure A.2.

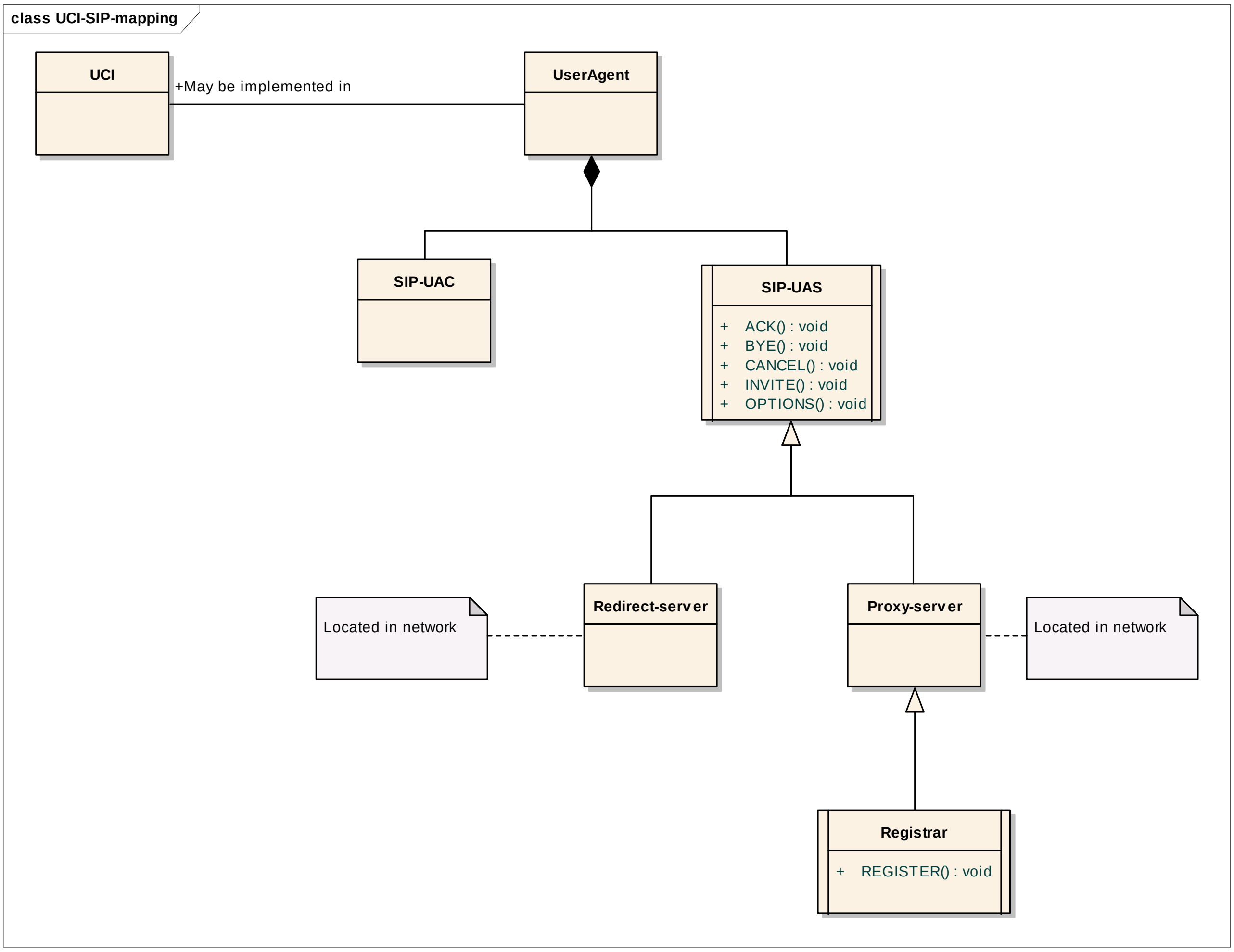


Figure A.1: UCI using SIP architecture

As shown in figure A.1 UCI may be implemented in a SIP User Agent and as such there is no distinction of PUA and SA functionality.

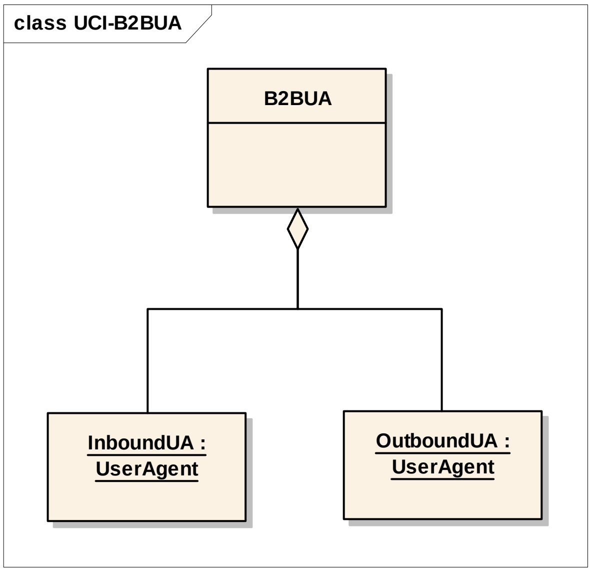


Figure A.2: NGN B2BUA as aggregation of user agents

A.2 Information element mapping

The username of a UCI user's SIP Address of Record (AoR) will be their UCI numeric, and the realm element of the AoR will be the realm that is providing UCI-related services to the UCI user e.g.:

- <my UCI-numeric>@myuciprovider.com

There are two major cases where the elements of the UCI, as described in clause 4.1.3, need to be mapped to elements of a SIP request:

- when a UCI user initiates a request.
    - This is the first operation in a user attempt to establish a communication session with a remote user;
- when a PUA is exchanging requests and responses with another PUA.
    - These are the steps in a communication session attempt that follow the initial UCI user to PUA request.

Tables A.1 and A.2 describe the mappings for these two scenarios.

In the case where UCI initiates a request the following options may apply:

1) The UCI user enters or selects a UCI SIP URI. This option has no implications and only requires basic and standard SIP behaviours.

2) The UCI only knows the UCI numeric of the target UCI user for the proposed session. In this case two options have to be supported:

    - the terminal or application supporting the SIP User Agent functionality is able to use a resolution service (ENUM) to resolve the target UCI-numeric to a SIP URI for the target UCI user. In this case the SIP User Agent can use the returned SIP URI as the destination SIP URI.

    - the terminal or application supporting the SIP User Agent functionality cannot or does not perform a resolution of the UCI-numeric. In this case the target UCI-numeric must be forwarded to the UCI user's PUA which can then perform the necessary resolution. This option ensures that UCI users will only ever have UCI-numerics and not UCI SIP URIs stored locally in their terminals and applications. This behaviour better supports the UCI goal of avoiding stored UCIs becoming invalid if the people referred to by those UCIs change the supplier of their UCI-related services (and hence their UCI SIP URI).

3) The UCI user enters a nickname for the target UCI user that is known to their PUA. In this case, the nickname must be transported to their PUA where a local lookup to resolve the nickname to a UCI-numeric is performed before the PUA uses the standard resolution service (ENUM) to resolve the UCI-numeric to a SIP URI.

An RFC 3261 [5] compliant information element mapping that supports the above options is shown in table A.1.

Table A.1: Information element mapping for when UCI users send requests to their own PUAs

UCI element	SIP element	Notes and observations
UCI-numeric	The UCI-numeric for the originator of the request will be the username part of the UCI user's AoR. It will thus appear as part of the From field. The UCI-numeric of the target user will appear as the username part of the Request URI and the URI in the To field.	The realm element of the Request URI and the To field will either be the valid realm of the target user or a dummy realm that the originating user's PUA will recognize and re-write into the valid realm for the target user. E.g. <UCI-numeric>@re-write-me.com Also, the username element of URIs using this dummy realm may be nicknames that the originating user's PUA will re-write into the UCI-numeric associated with that nickname. This is directly analogous to the use of dummy realms to support anonymous communication as specified in clause 8.1.1.3 of RFC 3261 [5].
UCI-label	User-specified, session specific, UCI-label information may precede the URI in the From field.	The UCI user may choose to specify a label that they wish to use for this session, in which case this should precede the URI in the To field. Otherwise, nothing should precede this URI. The UCI user's PUA will know from its internal rulebase which of the UCI-user's pre-defined set of labels to use in its subsequent transactions with other PUAs.
UCI- AdditionalData	This should appear as part of the message body of the request.	The format and content-type descriptions for the message body are FFS.

In the case where one PUA sends requests or responses to another, the mapping is as shown in table A.2.

Table A.2: Information element mapping for when PUAs sends requests/responses to other PUAs

UCI element	SIP element	Notes and observations
UCI-numeric	Request URI, To Field and From field.	The SIP URI of the request originator appears in the From field and the SIP URI of the target appears as the request URI in the To field. The user field of each of these SIP URIs will contain the appropriate UCI-numeric.
UCI-label	From field.	The UCI-label of the request originator may appear before the SIP URI in the From field.
UCI- AdditionalData	This should appear as part of the message body of the request.	The format and content-type descriptions for the message body are FFS. One element of the additional data will indicate whether the label that follows the SIP URI in the From field is an authentic UCI-label for that user.

A.3 Architecture mapping

Mapping the functionality of a PUA and SA to the logical entities described in RFC 3261 [5] is a non-trivial task and will require significant further consideration. One of the principal roles of the PUA is to:

- have access to and to interpret user profile information related to the UCI user;
- have knowledge of whether the target user is already known to the UCI user (i.e. is present in that user's contact book);
- have knowledge of whether, or not, the target user is using an authentic UCI-label (by examining SIP responses from the target user);
- make decisions about the information to be written into SIP request headers and message bodies as a result of evaluating user-supplied rules that operate on the above, and other, data.

Given that the PUA and SA combination may be responsible for significantly transforming an original user request before initiating a request to the PUA of the target user (see table A.2 in clause A.2), as well as by evaluating rules as described above, they may best be mapped as a Back-to-Back User Agent as defined in RFC 3261 [5].

Mapping the PUA and SA to NGN entities is also a non-trivial task. To aid the task, the key logical functional entities within a PUA have been identified and are shown in figure A.3. The functional entities have been chosen as those that would be needed to enable the PUA to perform all of the tasks that are stated or implied in the wide range of requirements and scenarios documented in the previous UCI documents EG 201 940 [1], EG 202 067 [2] and EG 203 072 [3].

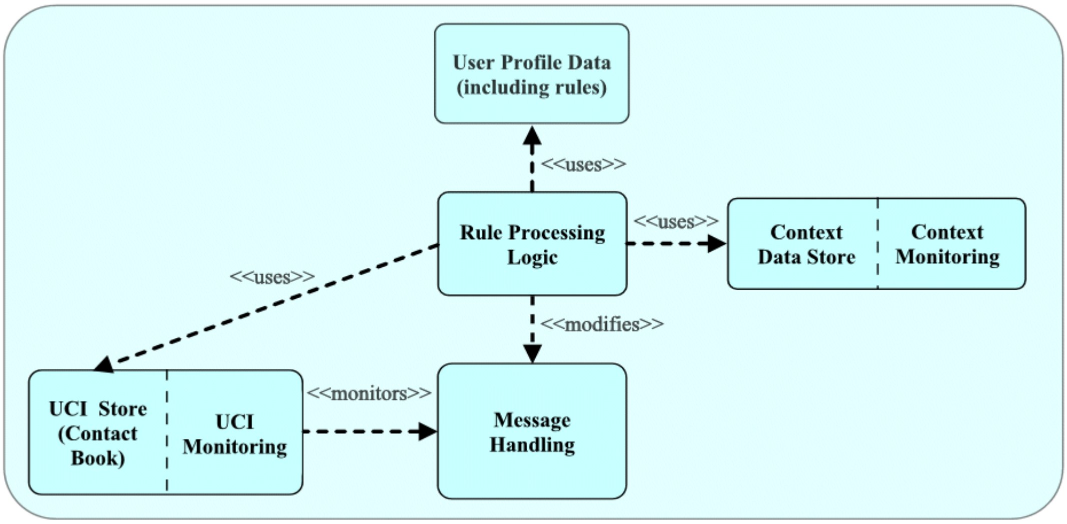


Figure A.3: PUA logical functional entities

As the PUA will be acting as a SIP server, the message handling element shown in figure A.1 will be realized as a CSCF. It will be a requirement that the S-CSCF and P-CSCF that are allocated to the UCI user will understand any UCI specific behaviours (e.g. the handling of a dummy realm as described in table A.1).

The PUA will be dependent for much of its intelligence on the processing of information from the user profile of the UCI user. The storage for the user profile data is shown in figure A.1 as the entity "User Profile Data (including rules)". As it is the UPSF that is responsible for user profiles, it has already been identified that the "User Profile Data (including rules)" functionality maps very closely to functionality in the UPSF (see clause 5.5 and figure 9). For UCI purposes, the types of user profile data held by the UPSF may need to be extended to include new types such as the user-supplied rulesets that are so essential to the effectiveness of PUAs.

As well as using user profile data, the PUA makes use of information about the current context of the user, including their current status and their willingness or ability to communicate. The PUA needs to access such information and store it for use when processing rules. The "Context Monitoring" entity in figure A.1 maps to the NGN Presence Server.

The PUA performs special processing that enables it to determine the appropriate header and message body data needed to establish an end-to-end user sessions that meet the requirements of both UCI users. This functionality is represented in figure A.1 as the "Rule Processing Logic" entity. Figure A.3 also identifies other entities that are related to the processing done by the PUA. These are shown in figure A.3 as:

- a "Context Data Store" to keep track of the current status of the different context sources (without having to poll for this data each time the PUA needs to take context into account);
- a "UCI Store (Contact Book)" for keeping a record of people or organizations familiar to the UCI user;
- a "UCI Monitoring" element that looks in the session setup dialogues for new UCIs that may require to be stored.

In carrying out all of the functions represented by the "Rule Processing Logic", "Context Data Store", "UCI Store (Contact Book)" and "UCI Monitoring" elements, the PUA behaves in a similar way to an AS. This is also identified in clause 6.2.

In the UCI architecture, the primary purpose of the SA is to interpret the session control messages going to and from the PUA into a form that matches the messages used in the underlying network or service being controlled. The entity in the PUA that sends and receives these messages is the "Message Handling" entity shown in figure A.3. As this is mapped to a CSCF in the NGN, there is no need for any interpretation to take place to enable the PUA to control NGN SIP based communication sessions. Therefore, for NGN based SIP sessions no SA is required. There are two instances in the NGN where interpretation will be required:

- when the target network/service uses ISUP (e.g. PSTN/ISDN);
- when the target IP network is not an NGN network or in any other case where an NGN Border Gateway Control Function (BGCF) is used;

In these cases, the NGN entities that provide the appropriate interpretation act as an SA for that type of service (see clauses 6.2.2 and 6.3 for details).

In summary:

- the PUA will have functionality that represents a combination of that defined for an CSCF (one or more of the S-CSCF, P-SCSF and I-SCSF), a UPSF, an NGN Presence Server and an ASF;
- in a SIP context where no BGCF is used, there is no need for an element to perform the functions of an SA;
- in other contexts, the NGN entities that are already defined for providing interpretation and gateway functions act as an SA for that context;
- no requirement to modify the standard protocols and interfaces between these entities in order to support UCI behaviours implemented using SIP has been identified.

A.4 Protocol mapping

The protocol example given in RFC 3261 [5] clause 4 identifies a simple Message Sequence Chart and the content of the initial INVITE message (the MSC from RFC 3261 [5] is shown in simplified form in figure A.4).

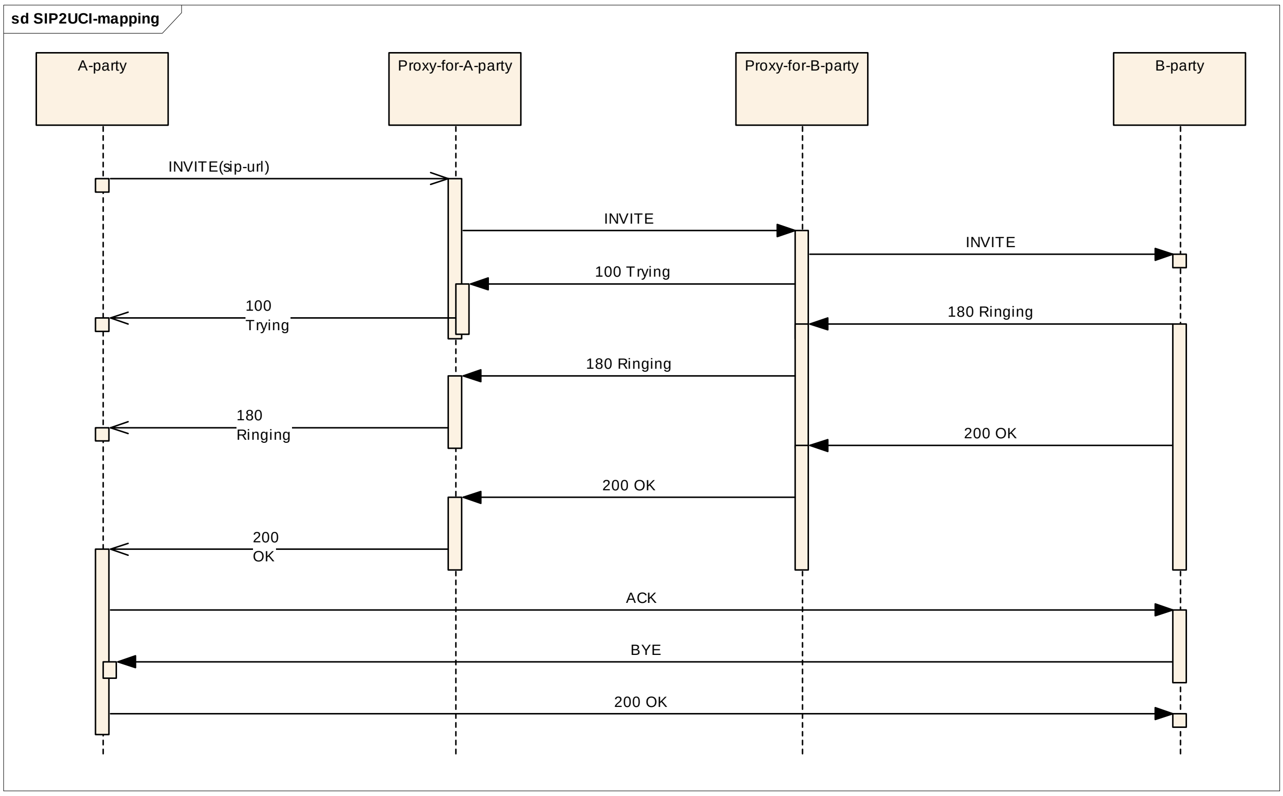


Figure A.4: Simple SIP message sequence chart

After a UCI user has registered with their PUA, UCI based communications can follow exactly this same message sequence chart, with Party A's PUA performing the Proxy-for-A-party function and Party B's PUA performing the Proxy-for-B-party function.

It is expected that assigning of the IMS elements that provide the PUA functionality will occur during IMS registration of the UCI user's terminals and applications.

As the dialogue between two PUAs is primarily aimed at the negotiation of an agreed set of parameters for a communication session.

All of the required features of dialogues between two PUAs should be achievable using standard SIP dialogues (similar to the example dialogue in figure A.4 but with messages such as "Ringing" being replaced with other confirmation messages).

The options described in table A.1 are illustrations of where initiation of sessions in a UCI context differs from the most basic form of SIP session initiation. Where the User Agent does not supply a fully qualified SIP URI as the Request URI (and To field), the PUA will be required to resolve the information supplied into the correct SIP URI of the target UCI (or non-UCI) user. The benefits derived from supporting this behaviour are related to supporting the UCI aim of protecting UCI users from losing contact with people in their address books when those people move to a new UCI provider - with a resultant inevitable change to the realm portion of their SIP URI.

Before initiating a dialogue with the remote user's PUA, the originating user's PUA may examine its user preferences and rules and determine pre-dialogue actions. The range of actions that the user's PUA could undertake are potentially limitless and could include things such as:

- warning the its user of reasons why they might not wish to proceed with the requested communication (e.g. the recipient is on a list of known fraudulent businesses, or, the user has a visitor arriving in 2 minutes);
- making modifications to the User Agent Capabilities that accompany the dialogue with the remote user's PUA e.g. a user with a sophisticated multimedia terminal might wish to have the User Agent Capabilities indicate that it was a voice-only terminal whilst the user was driving in their car.

It is neither possible to list all the operations that a PUA could undertake both before and during PUA to PUA negotiation as the majority of these are clearly outside the scope of standardization. However, any operation that does not break the SIP model or contravene the expectations of a well behaved SIP client/server should be permissible. The above two examples illustrate how clever features can be achieved without proposing any changes or additions to existing SIP specifications.

The end result of the dialogue between the two PUAs will be an agreed specification for the desired communication session that best meets the requirements of the two UCI users. In the simplest case this will have been achieved by a single INVITE followed by a 200 (OK) response as shown in figure A.1. Where the potential recipient may have many current constraints that limit what communications can be accepted, a sequence of multiple INVITES could take place that could ultimately end in a rejection message.

The final establishment of a communication session between User A and User B is initiated by User A's PUA. This will be based on the requirements determined during the PUA to PUA negotiation. The case where an entity (User A's PUA) initiates and controls a communication session between two users (User A and User B) corresponds exactly to the "third party control" situation addressed by RFC 3725. For this reason, it is recommended that PUA initiated communication sessions should follow the "best current practices" documented in RFC 3725.

The SIP INVITE message relating to the basic SIP scenario from RFC 3261 [5] (illustrated in figure A.1), is shown below:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

The first line of the text-encoded message contains the method name (INVITE). The lines that follow are a list of header fields. This example contains a minimum required set. The header fields and their probable role in deploying UCI with SIP are briefly reviewed in table A.3.

Table A.3: SIP header content mapping to UCI fields

Header name	SIP content	UCI mapping
Via	The address at which Alice is expecting to receive responses to this request. It also contains a branch parameter that identifies this transaction.	No special UCI mappings.
To	A display name (Bob) a SIP or SIPS URI towards which the request was originally directed.	When the User B is a UCI user, the SIP URI is their UCI SIP URI. The display name used may have no relationship with any variant of User B's UCI-label.
From	A display name (Alice) and a SIP or SIPS URI (sip:alice@atlanta.com) that indicate the originator of the request. a tag parameter containing a random string (1928301774) that was added to the URI by the softphone. It is used for identification purposes.	For all requests sent from User A's PUA, the display name will be a UCI-label associated with User A's UCI.
Call-ID	A globally unique identifier for this call, generated by the combination of a random string and the softphone's host name or IP address.	No special UCI mappings.
CSeq or Command Sequence	An integer and a method name. The CSeq number is incremented for each new request within a dialog and is a traditional sequence number.	No special UCI mappings.
Contact	A SIP or SIPS URI that represents a direct route to contact Alice, usually composed of a username at a fully qualified domain name (FQDN). While an FQDN is preferred, many end systems do not have registered domain names, so IP addresses are permitted.	No special UCI mappings.
Max-Forwards	An integer that is decremented by one at each hop.	No special UCI mappings.
Content-Type	Contains a description of the message body	No special UCI mappings.
Content-Length	Integer. contains an octet count of the message body.	No special UCI mappings.
NOTE 1: While the Via header field tells other elements where to send the response, the Contact header field tells other elements where to send future requests. NOTE 2: The combination of the To tag, From tag, and Call-ID completely defines a peer-to-peer SIP relationship between Alice and Bob and is referred to as a dialog.		

SIP User Agent (terminal) capabilities specifications according to RFC 3840 would appear to meet all of the currently identified requirements for conveying such information in both UCI user to own PUA and PUA to PUA requests.

RFC 2327 [22] appears to meet all of the currently identified requirements for conveying session type information between a UCI user and their own PUA and between PUAs.

A.5 Conclusion

At this level of analysis, standard SIP RFCs appear to provide the required functionality for PUA to PUA communication and for the establishment of communication sessions between UCI users. Also the way that SIP is supported in the NGN architecture also seems to provide the base level of support for the implementation of UCI in an NGN.

Annex B (normative): Mapping of UCI to NGN Presence Service

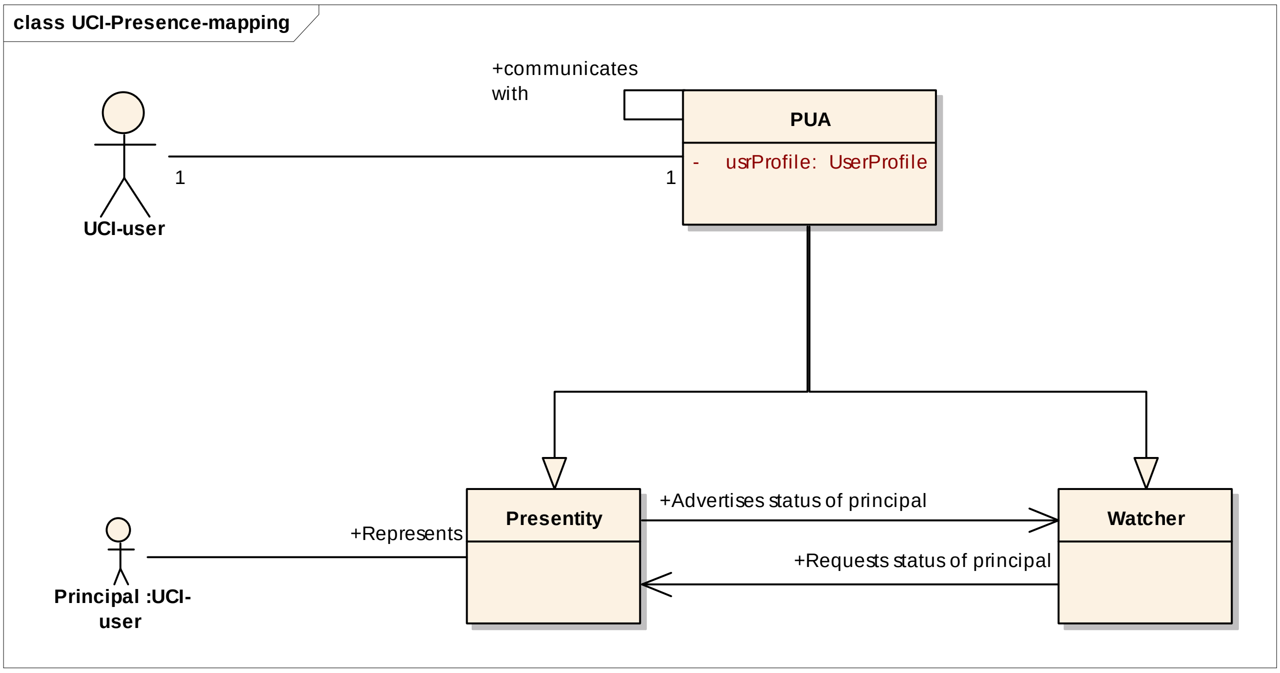
B.1 Overview

The effectiveness of the personalized management of a UCI user's communications environment will, to a very large extent, be dependent on three factors:

- the quantity and quality of the personal preferences configured by, or on behalf of, the user and stored in their user profile;
- knowledge of the people with whom the user wishes to communicate, in particular knowledge of their true identity;
- the availability of information about the status of the external environment of the UCI user, including the status of their communications services.

Obtaining the information described in the latter bullet will, predominately if not entirely, be achieved by means of presence services.

RFC 2778 [17] describes "A Model for Presence and Instant Messaging" that forms the fundamental model on which the NGN Presence Service is based. TS 122 141 [18] and TS 123 141 [19] are the Stage 1 and Stage 2 descriptions of the NGN Presence Service.


class UCI-Presence-mapping
+communicates with
PUA
- usrProfile: UserProfile
1
1
UCI-user
Presentity
+Advertises status of principal
Watcher
+Represents
+Requests status of principal
Principal :UCI-user

NOTE: The PUA may act as a presence server.

Figure B.1: Simplified presence relationships

B.2 Requirements mapping (from TS 122 141)

In UCI, it is the PUA that has the role of optimizing a UCI user's communications outcomes by using all the available information about the remote user, the UCI user and their environment. It is therefore the PUA that is identified as being responsible for gathering all relevant presence information.

The PUA has two fundamental presence related roles:

1) to gather presence information from all of the appropriate sources within and outside the UCI user's home environment;

2) to present a managed and unified presence view of the UCI user to other UCI users, to other NGN entities in the home environment and to external entities.

In the first role the PUA is acting as a presence watcher. The PUA may require presence information from a number of different sources and should be able to utilize standard presence mechanisms to obtain the required information.

TS 122 141 [18] defines two modes for obtaining presence information - Information Mode and Notification Mode. Information mode would be where the PUA requests the current presence information from a presentity. Notification Mode would be where the presentity notifies the PUA of changes in the presence state of the presentity.

It should be possible for the PUA to obtain presence information using both Information Mode and Notification Mode, but the use of these modes would need to be carefully planned to avoid creating a flood of presence update notifications. The following general rules could form the basis of a feasible model for managing presence in a UCI context:

- Information Mode would be an appropriate mechanism for the PUA to use to check the current status of presentities that are crucial to the success of the current transaction e.g. the PUA could check the current availability of a service that the PUA is planning to use to set-up a communication session;

- Notification Mode could be used to build a model of the current status of a number of less universally critical services that could influence the choices that the PUA makes. This would be very appropriate for services where the status changes very infrequently e.g. the time and location at which a user last drew money from an on-street cash machine (which gives location information when no mobile terminal location information is available).

The PUA will need to obtain information from a number of presentities both inside and outside the home environment. A principal source of presence information will be from the SAs that represent the UCI user's subscribed services. The PUA will need to know the presence identity of each presentity and separately subscribe to the presence information of these presentities.

The PUA will act in the role of an aggregator and redistributor of presence data from a number of presentities. It performs exactly the role described in clause 7.3 of RFC 3856 [24]. It will take presence data from a number of sources including:

- the presence information from its subscribed watchers;

- the current state of the user as derived from the application of the rules in the UCI user's user profile;

- any availability status that the UCI user wishes to declare in real-time (e.g. do not disturb);

and from these it will compute new presence information for the UCI user. The PUA will then be able to make this computed presence information available to other entities (watchers) as representing the current presence status of the UCI user (the principal). In this role, the PUA would be acting as presentity.

All of the above behaviour is consistent with the Stage 1 description documented in TS 122 141 [18].

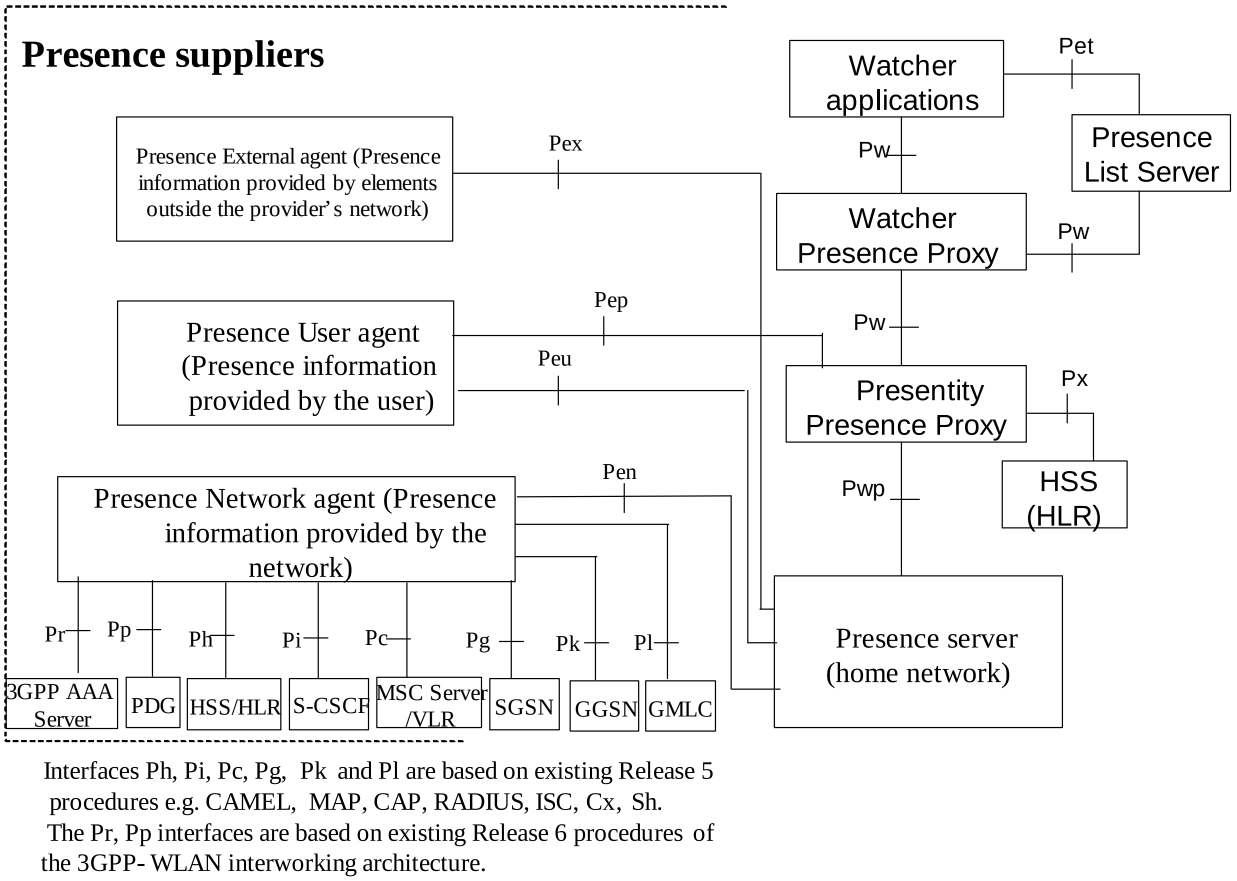
B.3 Architecture mapping (from TS 123 141)

Each PUA acts as a watcher and presentity simultaneously.

NOTE: In reading this clause, it should be noted that TS 123 141 [19] uses the abbreviation PUA to represent a Presence User Agent. In the context of the present document, the abbreviation PUA refers to a UCI Personal User Agent. Any references to Presence User Agents will use the full name of this entity and not its abbreviation.

As described in clause B.2, each PUA acts as a watcher and presentity simultaneously. The PUA is a watcher of any or all of the services that the PUA lists as being services used by the UCI user. The principal source of presence information will come from SAs. The user may have one or more different presence identifiers at each of the SAs. Each identifier will relate to the identity of the UCI user in that service. The PUA will maintain a record of all of these identifiers in order to subscribe to the presence information from those SAs.

In its role as a presentity, the PUA will present presence information to other entities. To achieve this, it will be necessary for the PUA to combine the presence information in potentially complex ways to produce a single picture of the UCI user's presence. This is the functionality of a Presence Server and TISPAN already defines an NGN Presence Server that is shown in figure B2.



Presence suppliers
Presence External agent (Presence information provided by elements outside the provider's network)
Presence User agent (Presence information provided by the user)
Presence Network agent (Presence information provided by the network)
Pex
Pep
Peu
Pen
Pr
Pp
Ph
Pi
Pc
Pg
Pk
Pl
3GPP AAA Server
PDG
HSS/HLR
S-CSCF
MSC Server /VLR
SGSN
GGSN
GMLC
Watcher applications
Pet
Presence List Server
Pw
Watcher Presence Proxy
Pw
Pw
Presentity Presence Proxy
Px
HSS (HLR)
Pwp
Presence server (home network)
Interfaces Ph, Pi, Pc, Pg, Pk and Pl are based on existing Release 5 procedures e.g. CAMEL, MAP, CAP, RADIUS, ISC, Cx, Sh.
The Pr, Pp interfaces are based on existing Release 6 procedures of the 3GPP- WLAN interworking architecture.

Figure B.2: Reference architecture to support a presence service (from TS 123 141 [19])

It appears that the NGN Presence Server has the functionality to allow it to perform most of the presence related tasks that UCI defines for the PUA. One of the most critical aspects of how a PUA is expected operate is that its behaviour is determined by user initiated rules about how they wish their communications to be influenced by presence information and how they want their presence information presented to other entities.

The UCI model assumes that there are rules in the user's user profile that set the policy for meeting the user's requirements. It will be important that using the NGN Presence Server does not undermine this objective. With regard to the Presence Server, TS 123 141 [19] states, in clause 5.1 that:

"The mechanisms for combining the presence related information shall be defined based on presence attributes and according to certain policy defined in the Presence Server".

In order that the functionality described in UCI documents can be achieved, it is important that the policies that are applied in the Presence Server to combine presence information related to UCI can be configured on a user by user basis in a dynamic way e.g. each user may have different requirements of how they wish their presence information to be derived and released and they will also need the facility to change the policies (rules) that control the way that their presence information is manipulated. TS 123 141 [19] makes many references to allowing entities to control subscription authorization, but no such statement is made regarding the "policy" for combining presence information from multiple sources referred to in clause 5.1 of TS 123 141 [19].

It is not clear from TS 123 141 [19] whether the planned capabilities of the NGN Presence Server will easily support the required user by user flexibility in defining and managing the policies for combining presence information. If it is not anticipated that this level of flexibility can be directly supported by the Presence Server, then there may be a need for a separate entity that can translate the separate user by user policies stored in user profiles and present the Presence Server with a single policy that it can utilize. This would be analogous to one of the options in clause 7 of TS 123 141 [19] for managing subscription authorization lists:

"The subscription authorization lists can be logically arranged to be part of the presence server or a separate entity in the network".

In all other respects, it appears from analysis that the Presence Service described in TS 123 141 [19] can support the presence requirements necessary to support UCI.

B.4 Protocol mapping

For UCI usage, the statements related to protocol in TS 123 141 [19] apply. In particular, TS 123 141 [19] states that multiple protocols should be supported in the presence service

As SIP has been identified as the most relevant protocol for the primary transactions between PUAs and between PUAs and SAs, the use of SIP to convey presence information, as described in RFC 3856 [24], would appear to be the most promising option for further investigation in terms of the presence flows into and out of PUAs and SAs. TS 123 141 [19] proposes the use of SIP as a key protocol to support presence between entities within the NGN.

Annex C (informative): Liberty Alliance Project Identity Federation Framework (ID-FF)

C.1 Overview

The Liberty Identity Federation Framework (ID-FF) contains the core specifications that allow for the creation of a standardized, multi-vendor, identity federation network. The Federation Framework consists of protocols, schema and profiles.

Federated Identity Management is one of the strategic objectives (known as "Federation") of the Liberty Alliance Project (http://www.projectliberty.org) that formed to establish an open standard for federated network identity.

The key objectives of the Liberty Alliance from [LAP1] are to:

- enable consumers to protect the privacy and security of their network identity information;
- enable businesses to maintain and manage their customer relationships without third-party participation;
- provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers;
- create a network identity infrastructure that supports all current and emerging network access devices.

These capabilities can be achieved when, first, businesses affiliate together into circles of trust based on Liberty enabled technology and on operational agreements that define trust relationships between the businesses and, second, users federate the otherwise isolated accounts they have with these businesses (known as their local identities). In other words, a circle of trust is a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment (figure C.1). It should be noted that Operational agreement definitions are out of the scope of the Liberty Version 1.2 specifications.

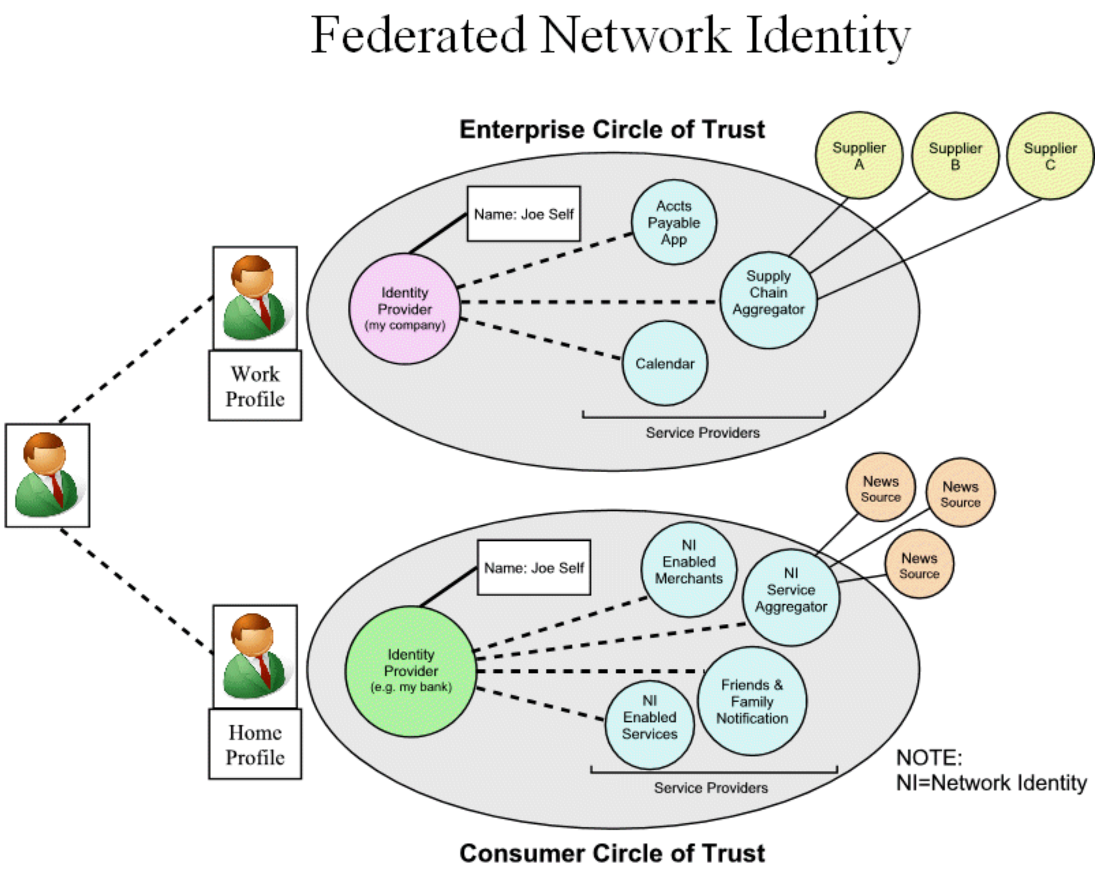


Figure C.1: Federated network identity and circles of trust

From a Liberty perspective, the salient actors in are the user, service providers, and identity providers.

Service providers are organizations offering Web-based services to users. This broad category includes practically any organization on the Web today, for example, Internet portals, retailers, transportation providers, financial institutions, entertainment companies, not-for-profit organizations, governmental agencies, etc.

Identity providers are service providers offering business incentives so that other service providers affiliate with them. Establishing such relationships creates the circles of trust shown in figure C.1. A single organization may be both an identity provider and a service provider, either generally or for a given interaction.

These scenarios are enabled by service providers and identity providers deploying Liberty-enabled products in their infrastructure, but do not require users to use anything other than today's common Web browser.

Federated identity allows users to "link" elements of their identity between accounts without centrally storing all of their personal information. The final version of federation specifications - ID-FF 1.2 was sent to OASIS for inclusion in SAML 2.0. Additionally, the support for SAML 2.0 has been developed in the Identity Web Services Framework standards, completing the cycle and offering a full solution to deployers.

The Liberty Alliance Identity Federation specifications now also part of the OASIS SAML 2 suite) support the possibility that a user can obtain access to multiple websites via single sign-on, and that an identity provider (IdP) may make an assertion of his authenticated status to its service provider partners in a circle of trust. Identity providers may also make other identity claims about someone, based upon information that a person has given them in association with that person's account held at the IdP. The user may control the behaviour of identity providers and service providers. For example, a service provider may accept assertions issued by one of several identity providers, and the user of the service provider can choose which identity to use. Or, the user can choose to be anonymous at the service provider.

The Liberty ID-FF and SAML 2 specifications also address a problem of making identity claims, i.e., an identity provider can make a claim of the authenticated status of a "security principal" (in many cases, simply a person) to service providers with whom the identity provider has some trusted relationship. In the Liberty specifications, the trust relationship between the service provider and the identity provider regarding these types of assertions is bi-directional - the identity provider wishes to know that the party to whom it is making an assertion is a party that it can trust, and vice-versa. In a case where the identity provider might be in some way (legally) liable for making this claim, this bi-directional trust is important.

In many cases, a user's web browser can be redirected from a service provider's website to the identity provider's site, without any action by the user. This can result in a loss of control over SSO by the user. An alternative to this process is for the web browser to advertise to a service provider that it can locate an appropriate identity provider, and act as an intermediary between the IdP and the SP. This is done using the Liberty-Enabled Client or Proxy (LECP) profile.

The pattern used in the LECP profile can be generalized to include the ability for a user-agent (a web browser for example) to provide all kinds of identity claims, under the direct control of the user. It should be noted that there is the difference between self-asserted claims and trusted-third-party-asserted claims. It should be noted that it can be, for example, software that is running directly on a person's mobile phone that can make identity claims. Such software could implement any of the services defined by the Liberty ID-WSF specifications, including an Authentication Service, Single-sign-on Service, Discovery Service or Personal Profile Service.

When an identity claim has been made, it may be important for a service provider to verify that claim, and to authenticate the presenter of the claim. Verification involves evaluating the evidence supporting the claim and determining whether that evidence is adequate. Such evidence may include an assertion stating essentially that "the presenter of this claim is who he says he is" - an authentication assertion. Thus, authentication of the presenter of the claim is an important piece of evidence supporting other claims made by that presenter. It should be noted that authentication assertion may have been produced by someone other than the presenter of the assertion. One way to verify certain properties of a claim (such as integrity of the data in the claim, or the authenticated status of the presenter of the claim) is a digital signature. This links the cryptographic key used to sign the identity claim with that identity claim. An assertion stating the user's authentication status will most likely be signed by the issuer of the assertion, linking it inextricably to the IdP.

To conclude, the Liberty ID-FF together ID-WSF specifications, by means of the LECP profile, and by the possibility to host identity services on client systems (such as personal computers and mobile phones) allow individuals to maintain some direct control over the release of identity claims. Furthermore, Liberty identity providers and service providers are free to offer facilities that allow their users some control over network-hosted personal identity data.

The Liberty specifications make appropriate use of existing technologies for anchoring trust in a networked environment (such as X.509 certificates and XML Digital Signature) but do not demand their use. Thus, in environments where it can be expected that such technologies are not deployed (such as in user-operated devices), it is still possible to deploy implementations of the Liberty specifications that allow an individual to maintain more control over his digital identity information.

C.2 Liberty Alliance ID-FF 1.2 Specifications

Liberty ID-FF Architecture Overview [LAP1] is a non-normative summary description of the Liberty ID-FF architecture, including policy and security guidance.

The overall Liberty architecture is composed of three orthogonal architectural components (figure C.2):

- Web redirection: Action that enables Liberty-enabled entities to provide services via today's user-agent-installed base.
- Web services: Protocol profiles that enable Liberty-enabled entities to directly communicate.
- Metadata and schemas: common set of metadata and formats used by Liberty-enabled sites to communicate various provider-specific and other information.

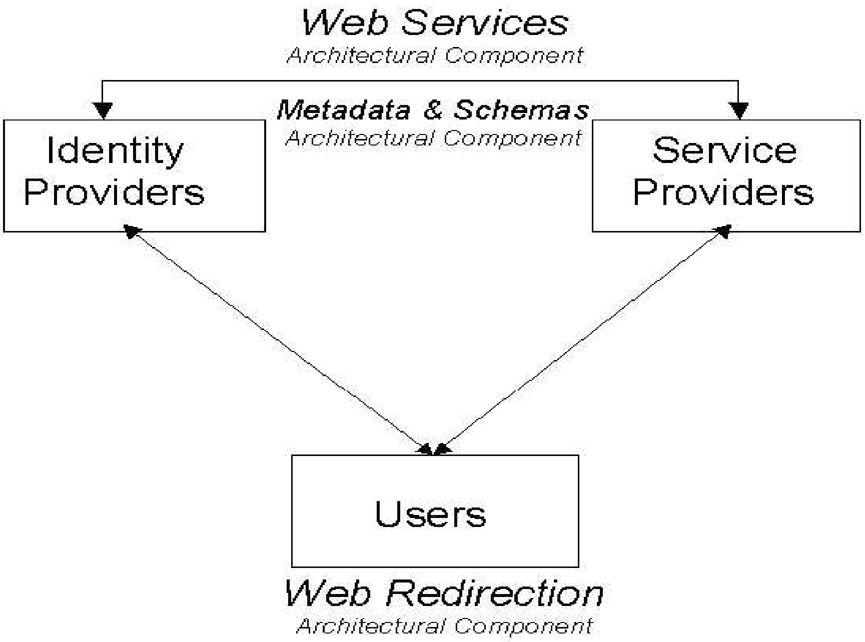


Figure C.2: Overall Liberty Architecture

Liberty ID-FF Bindings and Profiles Specification [LAP2] defines concrete transport bindings and usage profiles for the abstract Liberty protocols.

Liberty ID-FF Protocols and Schema Specification are involved in two documents. Abstract protocols and XSD schemas for Liberty are defined in [LAP3]. The XSD Schema that accompanies the Liberty Protocols and Schema Specification is defined in [LAP4].

Liberty ID-FF Guidelines [LAP5] defines the recommended implementation guidelines and checklists for the Liberty architecture focused on deployments for the service-providing entities: service providers, identity providers, and Liberty-enabled clients or proxies (LECPs).

Liberty ID-FF 1.2 Static Conformance Requirements, Version 1.0 [LAP6] defines what features are mandatory and optional for implementations conforming to this version of the Liberty Alliance Specifications.

Liberty ID-FF 1.2 Errata [LAP7] contains errata items pertaining to the Liberty ID-FF 1.2 specification set.

C.3 Liberty Alliance in a UCI context

In a UCI context, the Liberty Alliance work might be relevant when considering access to stored user profile information. Although the architectural diagram depicted in Figure10 in clause 6.2.1 shows what look like centralized stores of user profile data and identifies the actions undertaken by the PUA in the course of registration, there may be commercial and operational reasons why certain subsets of user profile data (and presence related data in some circumstances) may not be allowed to be held outside the domain in which it is initially stored (e.g. service related user profiles). Liberty Alliance solutions provide away of making distributed sources of user profile and presence data act, from the PUAs point of view, as if it was a single contiguous store.

Annex D (informative): Rationale for proposed UCI design options

D.1 Rationale for the design decisions behind the UCI-label

Even within a European context, the different elements of a personal name are varied and are interpreted differently from country to country. In the global context in which UCI must exist, the meaning of the elements of a personal name will be even more diverse [MISC1, MISC2]. For this reason, and because the label field may also contain information that includes company names, the UCI-label should be considered as a single unstructured alphanumeric string.

The content of the UCI-label and its formatting will be the responsibility of the UCI user. In principle the label may be any alphanumeric string. Given the international diversity of the content of a UCI-label, it is difficult to identify a maximum length for this string - or even to identify a typical range of lengths. A figure of 128 bytes has been suggested for a maximum length to handle personal names in [MISC2], but it would be wise to avoid unnecessarily constraining the length of the UCI-label.

The UCI alphanumeric label's primary role is to convey meaning to end-users. The UCI-label is the element that should be presented to an end-user during the setup phase of a communication session. It is the element that is most likely to convey to end-users the identity the other party and therefore allow the recipient to make decisions about how to respond to an incoming communication.

A single UCI user may have a number of different labels that they wish to be presented to another user, according to their current preference. User preferences may be implemented as rules to be followed by the UCI user's PUA and may be used to determine which label should be used according to factors such as:

- whether the person being communicated with is known to the UCI user;
- whether it will be a business or personal communication;
- etc.

The choice to use UTF-8 [MISC3] characters allows the string to be universally usable in all cultures. Some cultures may chose to have different variants of their labels available for sending to the other party (e.g. a label in Kanji for use when communicating with Japanese colleagues and one in Latin script for use in other circumstances (both could be certified as authentic). This reflects current practice in the use of business cards. The UCI user's PUA could chose which label to use dependant on the identity of the recipient.

The principle identification features offered by use of the UCI-label are:

- the ability to present highly relevant information about the UCI user, to a remote party, by means of a label;
- the information in the label can be the same irrespective of the communication or information service being used;
- the remote party's PUA can establish the best way to present the UCI user's label information (e.g. the textual label may be spoken to the remote user by invoking a text to speech service if the remote user has no visual display, or if they have poor vision, or if they are driving);
- the UCI user can choose to present different label information according to the context in which the label will be used (e.g. in a chat room an alias may be used, whereas an "authentic label" may be used to establish credibility and trust);
- the label that is presented to the remote user may be selected by a rule that is running in the UCI user's PUA;
- UCI-labels may be stored by the UCI user's PUA, constructed by means of PUA rules, or generated by the UCI user for a specific usage instance;

- "authentic labels" are labels that have been certified by a trusted third party as being an accurate identity for the UCI user (e.g. the UCI user's official name that was registered at birth or a name by which the UCI user is commonly known);
- "authentic labels" cannot be modified by the UCI user once they have been certified.

D.2 Why UCI information should be delivered by the UCI user's own PUA

The rationale for recommending this approach is:

- in UCI-based communication, the PUA will always have received the UCI-numeric and UCI-label that needs to be delivered;
- a PUA will have extensive presence derived knowledge of the capabilities of communications services, access networks and devices available to its end user. This would allow the PUA to determine a suitable method to deliver the UCI-numeric and UCI-label to its end-user - even making use of a different service and/or device to deliver the notification to those being used to receive the communication;
- in international communication, where a telephony call may transit a number of countries, no guarantee can be given that the identity carrying CLIP/OIP in [MISC4, MISC5] information (or COLP/TIP in TS 183 008 [8] information) will successfully reach the other end;
- in many corporate environments, a corporate network may replace CLIP information related to the end-user with information relating to a generic company contact point;
- commercial, internet-based, services already exist that are explicitly marketed as a way for a person to send false CLI information to the PSTN or PLMN with whom they wish to talk;
- in order to ensure that a return communication can be made, PUAs must have a means to ensure that the UCI-numeric can be delivered irrespective of the communication service or terminal type. As the PUA is ultimately responsible for protecting and managing identity issues for the user across all forms of communication, it is logical to see it as the point of first responsibility.

D.3 The benefits of a single identifier associated with tight control of incoming communications

One of the goals of UCI is to allow the user to establish more control over their communications environment and to protect themselves from unwanted communications via a number of independent alternative paths e.g. mobile phone, fixed phone, email, IM. When Person A knows the service related identifier of Person B, Person A can attempt to contact Person B in an unrestricted manner using that service. The more a person's identifiers across a range of services are made available, the more vulnerable to unwanted communications they become.

The UCI concept of having a single identifier (or very restricted number of them), that works for all services, and that is associated with sophisticated control mechanisms, was a direct response to the flood of unwanted communications scenario. This approach supports:

- identifying unknown callers who are unwilling to reveal their true identity (this will help to target commercial cold-calling where a retail organization pretends to be a research organization);
- clearly identifying known callers (who can then be given preferential access to the UCI user);
- limiting access via certain communication channels to times when this access is socially acceptable (e.g. no phone calls at night except from close family and friends);
- etc.

Annex E (informative): Bibliography

E.1 Liberty Alliance Project

The specifications mentioned are available from:
http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[LAP1] Liberty ID-FF Architecture Overview: draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf .

[LAP2] Liberty ID-FF Bindings and Profiles Specification: draft-liberty-idff-bindings-profiles-1.2-errata-v2.0.pdf .

[LAP3] draft-liberty-idff-protocols-schema-1.2-errata-v3.0.pdf.

[LAP4] liberty-idff-protocols-schema-1.2-errata-v3.0.xsd.

[LAP5] Liberty ID-FF Guidelines: liberty-idff-guidelines-v1.2.pdf.

[LAP6] Liberty ID-FF 1.2 Static Conformance Requirements, Version 1.0: liberty-idff-1.2-scr-v1.0.pdf.

[LAP7] Liberty ID-FF 1.2 Errata: draft-liberty-idff-1.2-errata-v1.0.pdf.

[LAP8] Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, March 2003.

E.2 ETSI UCI documents

[UCI1] ETSI EG 202 249: "Universal Communication Identifier (UCI); Guidelines on the usability of UCI based systems".

[UCI2] ETSI EG 202 301: "Universal Communications Identifier (UCI); Using UCI to enhance communications for disabled, young and elderly people".

[UCI3] Pluke, M, et al. (1993). "Bringing benefits to the disadvantaged by providing flexibility for all", 20th Symposium on Human Factors in Telecommunications, HFT03, Berlin.

[UCI4] Pluke, M. (1994). "ETSI's Universal Communications Identifier (UCI) - from its origins to its diverse benefits", Telektronikk, 1.2004.

E.3 IETF documents

[IETF1] IETF RFC 2916: "E.164 number and DNS".

E.4 Miscellaneous documents

[MISC1] "Handling People's Names", Guidance information from the Inter-Locale LLC website (http://www.inter-locale.com/Names.html).

[MISC2] "What's in a Name?", Tutorial presented at 26th Internationalization and Unicode Conference, San Jose, USA, September 2004 (http://www.inter-locale.com/whitepaper/IUC26-a302-Names.pdf).

[MISC3] Unicode Consortium standards (http://www.unicode.org/).

[MISC4] ETSI EN 300 089: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Service description".

[MISC5] ETSI TS 183 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

[MISC6] ETSI EN 300 094: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Service description".

[MISC7] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[MISC8] ETSI TS 102 051: "ENUM Administration in Europe".

[MISC9] ETSI TS 102 172: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Minimum requirements for interoperability of ENUM implementations".

History

Document history		
V1.1.1	July 2007	Membership Approval Procedure MV 20070907: 2007-07-10 to 2007-09-07
V1.1.2	September 2007	Publication