Final draft ETSI EG 202 067 V1.1.1 (2002-07)

ETSI Guide

Universal Communications Identifier (UCI); System framework

Reference

DEG/HF-00025

Keywords

addressing, 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

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

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

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

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2002.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 Human Factors (HF), and is now submitted for the ETSI standards Membership Approval Procedure.

Introduction

EG 201 940 [1] introduced the concept of a Universal Communications Identifier (UCI) to provide a flexible means of identification in an increasingly communications intensive world. To achieve its full potential the UCI needs to operate within an architecture capable of supporting the concept of personal control of communication.

The UCI being used within the architecture described in the present document overcomes the many limitations that arise from the use of the identifiers in current communications systems. When the UCI is used it:

- can identify the user in a meaningful way;
- minimizes the need to for a user to have many different identifiers for a range of different communications services;
- provides the potential for verifying the true identity of the originator or recipient of a communication;
- is unchanged when moving to a different service provider or service type; and
- may provide a common environment for the management and control of all personal communications irrespective of service type (as opposed to a range of different control mechanisms that are service specific).

The UCI may offer additional benefits arising from the application of rules stored in a personal profile contained in a Personal User Agent (PUA). These rules operate with a wide range of information including:

- the identity (UCI) of people attempting to communicate with the user;
- the date and time when communication is attempted;
- the location of the user;
- the urgency of the communication;
- whether the originator of a communication has a work or a personal status; and
- the user's preferences for how they wish to be reached (which services and which terminals).

The operation of these rules can permit a very high degree of control over the user's communications. EG 201 940 [1] gives some scenarios illustrating the potential power and flexibility of UCI-based communication. Further examples are given in more detail in annex A.

Parts of the present document, in particular the scenarios, imply a great deal of complex rule driven behaviour. This behaviour would come from advanced PUAs intercommunicating. In the early phases of UCI it is possible that not all PUAs will support such behaviour.

1 Scope

The present document:

- defines the system architecture and operations needed for a Universal Communications (UCI) implementation capitalizing on existing and emerging standards;
- identifies and documents the standards that are available (or that will be available) to enable the UCI to be implemented.

In line with the above one of the prime requirements during development of the UCI concept has been to minimize the number of specialized technical requirements necessary for its implementation. Similarly the assumption has been that most of the functionality necessary to put UCI into practice will appear as part of the natural evolution of a future communications network architecture (the rapid evolution of services such as Presence and Location Based Services indicate that this assumption is realistic).

With regard to standardization, the approach taken has been to avoid promoting the creation of new standards solely for the purpose of creating UCI systems when existing or developing standards can be used, amended, or extended.

The main UCI functional entities are described in clause 6. Clauses 7 and 8 describe the required capabilities of UCI systems and list the technical requirements for UCI. Details of UCI dialogues, services, processes are contained in clause 9. Descriptions of communication using UCIs and of how UCI assists in personal privacy protection follow in clauses 10 and 11. Descriptions of the data handled in UCI systems and a UCI Security Framework are in clauses 12 and 13. Finally, in the main document, a brief introduction to UCI administrative issues and to the principal standards that could support UCI are contained in clauses 14 and 15.

Annex A contains a number of scenarios that illustrate the UCI being used in everyday tasks. Each scenario describes how UCIs might be used in realistic communications related situations. Both the user experience and key elements of underlying system behaviour that produces that experience are shown. The scenarios:

- show how meeting the user requirements described in Annex B enables realistic and powerful usage scenarios to be delivered;
- help to identify and validate the system capabilities that are needed to deliver the required behaviour of UCI-based communication.

Annex B contains a systematic analysis of the user requirements (first defined in EG 201 940 [1]) which have been used to define the UCI architecture. Each requirement is described in detail with particular reference to which requirements are mutually supportive and which are potentially in conflict.

Annex C lists Standards Bodies which are potentially related to the UCI Technical Requirements.

Annex D gives a summary of security mechanisms that may be of relevance to UCI.

Annex E is a security risk assessment of UCI, primarily from the end-user security perspective.

Annex F draws comparisons between UCI and ENUM.

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.

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

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

[3] IETF RFC 2267: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing".

[4] IRTF RFC 2409: "Internet Key Exchange (IKE)".

[5] IETF RFC 2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[6] IETF RFC 2412: "The OAKLEY Key Determination Protocol".

[7] IETF RFC 2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[8] Krawczyk H: "SKEME: a versatile secure key exchange mechanism for Internet". IEEE Proceedings of the Symposium on Network and Distributed System Security, 1996.

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

[10] IETF RFC 2779: "Instant Messaging / Presence Protocol Requirement".

[11] IETF RFC2644: "Changing the Default for Directed Broadcasts in Routers".

[12] "PAM Specification v1.0"; PAM Forum; latest version available from.

[13] ETSI ES 201 915: "Open Service Access (OSA); Application Programming Interface (API)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

electronic signature: evidence in a digital form that can be processed to get confidence that some commitments has been explicitly endorsed under a Signature Policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally role

security association: set of policy and key(s) used to protect information

NOTE: The ISAKMP [5] [7] Security Association is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication.

signature policy: set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid

social protocols: mediate interactions between humans using computers/networks, or computer agents acting on behalf of human concerns

3.2 Abbreviations

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

AH	Authentication Header
AI	Artificial Intelligence
API	Application Programme Interface
CLI	Calling Line Identity
CNIP	Calling Name Identification Presentation
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENUM	Electronic Numbering
ESP	Encapsulating Security Protection
FIPA	Foundation for Intelligent Physical Agents
GSM	Global System for Mobile communication
ID	IDentifier
IETF	Internet Engineering Task Force
IF	Information Flow
IKE	Internet Key Exchange
IM	Instant Messaging
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol (IETF)
NAPTR	Naming Authority Pointer
PAM Forum	The Presence and Availability Management (PAM) Forum
PSTN	Public Switched Telephone Network
PUA	Personal User Agent
PUA_o	Personal User Agent [originating]
PUA_r	Personal User Agent [recipient]
SA	Service Agent
SA_o	Service Agent [originating]
SA_r	Service Agent [recipient]
SIM	Subscriber Identification Module
TETRA	Terrestrial Trunked Radio
TMSI	Temporary Mobile Subscriber Identity
T_o	originator's Terminal
T_r	recipient's Terminal
UCI	Universal Communications Identifier
UCI_o	Originating UCI
UCI_r	Recipient UCI
USIM	UMTS Subscriber Identification Module

4 Void

5 The Universal Communications Identifier (UCI)

The UCI is a single, unique identifier for a user.

The UCI is a 3-part construct:

- a numeric identifier (globally unique);
- an alphanumeric label;
- an additional information field (not seen by communicants).

The numeric part of the UCI is unique and would be allocated by a trusted authority. One characteristic that it should exhibit is stability, i.e. it would not change over time even with a change of service provider.

EXAMPLE: Unique numeric identifier: 8837460633789;
Alphabetic label: John Smith;
Additional information: a6;f1;d234;k78 (see clause 7.4, SC 4.3)

Some of the key characteristics of the UCI include:

- it is a unique identifier for a person, role or organization;
- it allows a label to be used as a "user-friendly" name that describes the originator and/or recipient of a communication;
- it allows important additional information to be available to anybody using it, such as preferred language, acceptable languages, whether business/personal, label authenticity or alias, etc;
- it allows the originator or recipient of a communication to claim authenticity for their identifier;
- where it is particularly important to claim authenticity, additional procedures can be invoked to make sure that it is not another person using the terminal and thus not the person it seems to be;
- it is independent of services and networks;
- it is independent of service provider.

6 UCI functional entities

In the UCI system, every user role has an associated Personal User Agent (PUA), and every service has an associated Service Agent (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.

Clauses 6.2 to 6.4 give a brief description of the main system components associated with UCI systems.

6.1 UCI system overview

Figure 1 shows a simplified overview of how the UCI system components are used in basic communication set-up. Clauses 9 and 10 show more detail of the actual information flows that take place.

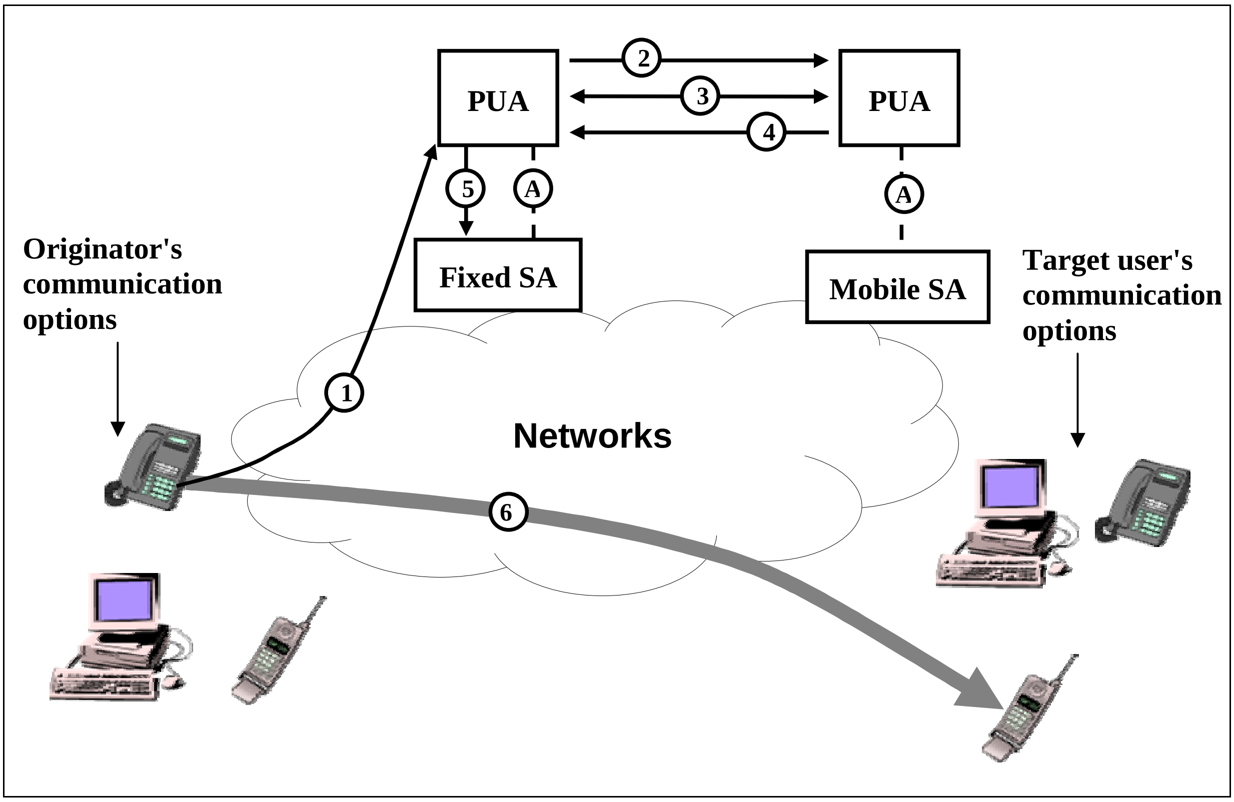

PUA
PUA
2
3
4
5
A
A
Fixed SA
Mobile SA
Originator's communication options
Target user's communication options
Networks
1
6

Figure 1: Simplified overview of UCI operation

Figure 1 shows a basic UCI communication scenario where the originator requests a voice call to the target user. The numbers and letters below refer to the numbers and letters labelling the flows in figure 1:

A) Each PUA may exchange information with the SAs of its user's networks/services at any time. The target user's PUA knows that the user's mobile phone is able to receive voice calls.

1) The originating user enters the UCI of the target user.

2) The originating PUA makes a request to the PUA of the target user.

3) The PUAs negotiate communication options if necessary.

4) The target user's PUA takes account of it's user's preferences and proposes the user's mobile phone to receive the call.

5) The originator's PUA instructs the originator's network to set-up the call.

6) A voice call between the originator's ISDN phone and the target user's mobile phone is established.

6.2 The Personal User Agent (PUA)

A PUA is a functional entity (probably implemented as a software object) 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, etc.). 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, etc.). Such data may be implemented using the presence and availability protocols defined by the Internet Engineering Task Force (IETF) in IETF RFC 2778 [9] and IETF RFC 2779 [12] and by the PAM Forum [10].

A PUA only 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.

6.3 The Service Agent (SA)

An SA is a functional entity that is linked to a communication service (or network). It would typically be provided by a network or service provider. An SA is the link between the UCI and networks and services. It participates in communication with PUAs, other SAs and its own network/service and would be specially trusted by PUAs following successful registration.

The SA provides a consistent interface to the PUA irrespective of the internal architecture of its network/service. Where the network/service already has entities that provide a common point of control over the network/service functionality, the SA merely provides an interface to these control functions that implements the API/protocols used by PUAs. Where the network/service does not provide such a common point of control, the SA must also provide additional functionality that interfaces with the distributed control mechanisms within the network/service.

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.

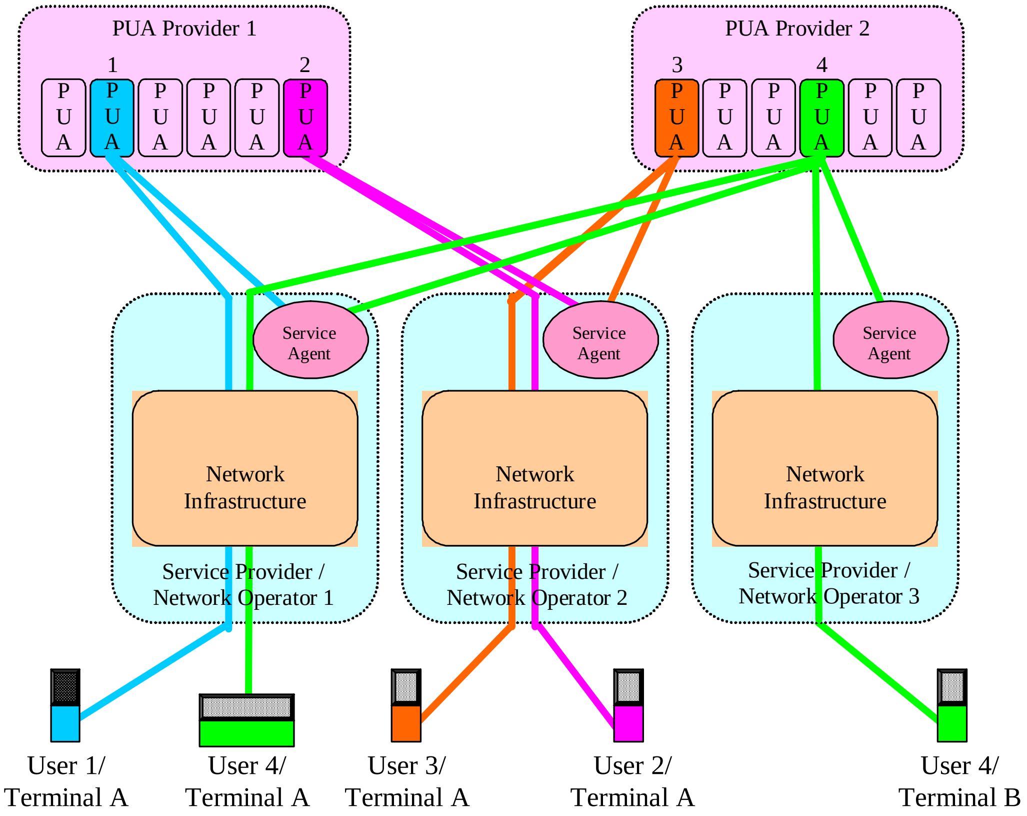


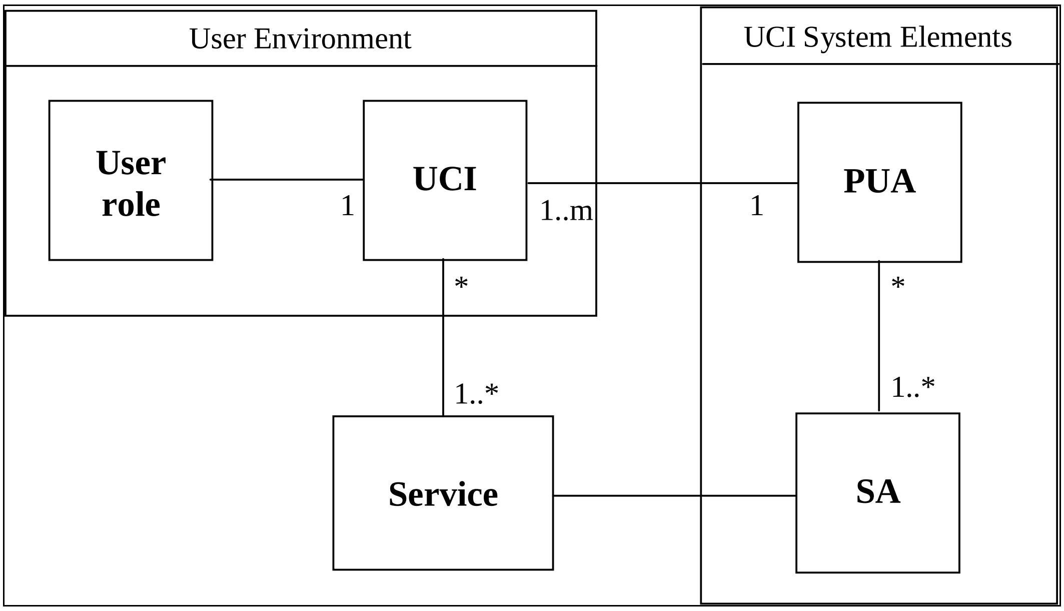
Figure 2: UCI Context Model

Figure 2 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.

6.4 Relationships between principal UCI entities

Each UCI user needs to register with their PUA in order to begin interacting in the UCI environment (for person-to-person communication or for communication management). In order that networks and services can be utilized to establish communications sessions, the PUA needs to identify an appropriate SA for that session and a registration needs to take place between the PUA and the SA. This registration process is shown in clause 9.3.1.

Figure 3 shows the multiplicity relationships between the principal UCI entities.



NOTE 1: In UML the "*" character represents an unlimited non-negative integer (including zero).

NOTE 2: For any instance of registration a service is associated with only one SA (i.e. n=1).

NOTE 3: A single PUA may have 1 or more UCIs (typically these would relate to "m" different roles for the same individual).

Figure 3: Class diagram of the principal UCI entities

The labelling of the multiplicity relationships in figure 3 shows that, for example, a service (participating in UCI) must have at least one SA but can have many SAs. Similarly it shows that several UCIs may be associated with a PUA but that one user role can only have a single UCI. What the diagram does not show is that because humans can have several life roles, they may have a number of UCIs that correspond to each of the life roles that they define.

6.5 Other entities

However, additional entities have been considered in the analysis of system capabilities in clause 7. These additional entities are:

- Terminals and end-user applications.

- These entities play an important part in the use of UCIs, but they are outside the main UCI context. However, broad implications for terminal design and functionality appear in the system capabilities (see clause 7) and technical requirements (see clause 8).

- Administrative entities.
  These will also need to be carefully considered in the analysis of the UCI architecture. An initial approach has been to assume that there may be a need to define number of different administrative entities, each entity being responsible for a single administrative role. This approach makes it easy to map to situations where a single business undertakes several administrative roles. Where the architecture assumes that a single business undertakes a number of roles it is much more difficult to map to an environment where for various reasons (e.g. the regulatory environment) the common ownership of these roles is not possible. The roles have not been looked at in detail yet, but they will play an important part in relation to issues such as the authentication of PUAs and SAs and in the provision and management of UCIs.

7 Capabilities for UCI-based communications systems

To meet the user requirements defined in annex B (derived from those first presented in EG 201 940 [1]), communications systems will have to provide specific capability.

The facilities available from PUAs will be subject to market forces. Some could provide a basic level of service; others could be more sophisticated with inbuilt Artificial Intelligence (AI) to predict user needs, etc. The following functions represent basic user requirements that should be met in all communication systems utilizing a PUA.

This clause lists these system capabilities. For each system capability, a list is provided indicating which user requirements it supports and with which other system capabilities or user requirements it might conflict. The impact of the system capabilities listed in terms of technical requirements is assessed against the architecture elements described in clauses 6.1 to 6.4.

7.1 System capabilities related to user input/output

SC 1.1 Providing user profile status

Users will have the opportunity to create a "user profile" and configure their communications in a potentially complex way. Routing of communications could be dependent on a wide range of factors such as the date, the day, the time of day, the urgency of the call, whether business or personal and so on. It is important that the user is able to interrogate the Personal User Agent and ascertain the current communication configuration.

System capability No SC 1.1 - Providing user profile status

The system should provide an indication of the current user profile.

Supports	UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR 1.8 - Trust in the system UR 2.2 - Ease of use SC 3.3 - Providing confidentiality/privacy of stored personal data
Requirements analysis	PUA - Capability to provide user configuration information in a form which can potentially be delivered on a wide range of terminals (e.g. web interface or speech interface) Terminal and local applications - Maximum support for PUA interrogation (e.g. function buttons and/or applications

SC 1.2 Editing the user profile

Given the complex user profiles achievable with new architectures, the user will inevitably wish to make changes. These could entail over-riding the default behaviour of the Personal User Agent for a specific communication, temporary changes to the profile, (e.g. going away on business for two days) or a permanent amendment to the profile (e.g. renting an extra fixed telephone line). The potential complexity of the user profiles means that the user interface to the communication management program is critical.

System capability No SC 1.2 - Editing the user profile
The system should provide the capability for users to easily edit their user profile.

Supports	UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR 2.2 - Ease of use SC 3.3 - Providing confidentiality/privacy of stored personal data
Requirements analysis	PUA - Capable of editing user configuration information. The amount of editing that can be done may vary according to the terminal type (e.g. full editing only from a web interface) Terminal and local applications - Maximum support for PUA editing (e.g. function buttons and/or applications)

SC 1.3 Availability of communication records

All proprietary email programs offer a communication history option. Most Telecommunications Companies also provide an outgoing call record if requested. Any future systems based on converging networks should offer the possibility of an integrated log for both outgoing and incoming communications managed by the Personal User Agent.

The communication records will act as a valuable source of UCIs that can be used for return communications or updating an address book. So, for example, the record of an email communication in history list can be used in the initiation of a telephone conversation with the email originator.

System capability No SC 1.3 - Availability of communication records
The system should provide for the delivery of a full communication history.

Supports	UR 2.2 - Ease of use UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR1.8 - Trust in the system
Requirements analysis	PUA - This would be the repository for the user's communications history across all services SA - When user communicated with a non-UCI recipient the users PA would not actively be involved in the communications set-up. In this instance the SA will inform the PUA that a communication has been made

SC 1.4 Access to personalized list of known UCIs

User identifiers will typically be stored in local or network based address books and Personal User Agents could have access to data from both sources. The source of data for the address books will be incoming communications, Smartcards and directories. Manual entry will also be required.

Users may require shared access to a group of UCIs (e.g. family members who have a common set of acquaintances).

System requirement No SC 1.4 - Access to personalized list of known UCIs
The system should maintain and provide User access to an address book of user identifiers. This may require duplication of this information in more than one physical or virtual location.

Supports	UR 1.3 - Increasing the options available to the originator UR 1.7 - Provision of a Universal Communications Identifier
Possible conflicts	None
Requirements analysis	PUA - continuously compiles a list of UCIs derived from incoming and outgoing communications plus search results. Able to synchronize with other PUAs, terminals and applications Terminals and local applications - Need to be capable of synchronizing with PUAs

SC 1.5 Determining a UCI (if unknown) by means of a search process

The originator will require that UCIs are obtainable by means of a search facility (access to any specific UCI may be restricted by its owner's privacy requirements). The originator's search query should be able to include various attributes such as:

- real name;
- "known as" name;
- current address;
- date of birth.

NOTE: These are examples of attributes that the searching user might use if they know them already. These attributes would not normally be made available otherwise.

System requirement No SC 1.5 - Determining a UCI (if unknown) by means of a search process
The system should provide access to a global search mechanism (or directories) for finding UCIs.

Supports	UR 1.3 - Increasing the options available to the originator UR 1.7 - Provision of a Universal Communications Identifier
Possible conflicts	SC 3.3 - Providing confidentiality/privacy of stored personal data UR 2.1 - System performance
Requirements analysis	PUA - Able to initiate a search and receive results from a directory service or other PUAs Terminals and local applications - Optionally provide enhanced search interface

SC 1.6 Selecting communication medium and characteristics

Currently the medium for a communication is determined by the terminal used by the originator and the identifier which is input (e.g. mobile number, email address). Evolving systems will be far more flexible and the Personal User Agent will need to know the preferred medium for each communication. Determination of the medium of choice could be determined by which terminal is being used, by a previously defined default option or by explicit selection (pointing to an icon on screen). Originators may also wish to specify the bandwidth or quality of a communication.

System capability No SC 1.6 - Selecting communication medium and characteristics
The system should provide the ability to select a communication medium as a user's first choice and specify attributes associated with that medium.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	SC 2.3 - Establishing contact where possible
Requirements analysis	PUA - May assume a default communications medium and characteristics based on the type of terminal contacting it. Must be capable of accepting instructions from the user via the same or different channel to the required communications channel Terminals and local applications - May have a default communications medium and characteristics. May allow the user to select alternative services and characteristics. Should be capable of overriding the default assumptions of the PUA

SC 1.7 Providing cost information

Users currently have little advance information, other than experience, on the potential cost of a call. Sometimes there are clues in a telephone number, the most obvious of which are freephone numbers. In a network of increasing complexity and with identifiers that give no clue as to physical distance, the ability to predict the cost of a communication will be further reduced. There will be occasions when an originator will wish to know the cost of a special call (e.g. videotelephony to another country) in terms of the rate/minute (before the communication), accumulating cost (during the call) or the total cost (after the communication).

System capability No SC 1.7 - Providing cost information
Originators of communications may request that tariff information is made available to them by the system so that they can predict the cost of a communication. Alternatively they may require that the accumulating or final cost be presented.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	None
Requirements analysis	SA - Provide charge detail records to PUA of resources used PUA - To allow interrogation of charge details

SC 1.8 Assign priority to communication when necessary

Apart from emails it is currently impossible to impart any urgency to a communication. For example, diversion of all calls to a mailbox or answering machine means that urgent calls are treated in the same way as non-urgent calls. This is clearly not an ideal situation. In future systems there is no reason why communications could not be allocated a priority where necessary and treated accordingly by the recipient's Personal User Agent. Such a priority request could not be guaranteed to be satisfied as it would be subject to the requirements of the recipient.

System capability No SC1.8 - Assign priority to communication when necessary
The system should provide the ability to assign "priority" to any communication.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	None
Requirements analysis	PUA - Originating PUA to communicate priority to receiving PUA SA - Urgency acknowledgement and suitable reaction Terminal capability of specifying priority (e.g. special function button)

SC 1.9 Providing originator anonymity

The subject of anonymity is a contentious one but few would argue against it being an essential provision when considering support lines for victims of crime or help lines for those who are suicidal or on drugs. A less dramatic example of where anonymity may be required is when an enquiry communication is made to a business and the enquirer does not wish the business to make follow-on communication attempts designed to secure a sale.

NOTE: There may be a requirement for Emergency Services to be able to identify the originator of a communication even when the originator has chosen to be anonymous.

System capability No SC 1.9 - Providing originator anonymity
The system should provide the option of originator anonymity when establishing a communication.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	SC 3.5 - Assuring identity
Requirements analysis	PUA - Instruct to communicate anonymously. Provide the capability of negotiating with the recipient PUA without disclosure of originating UCI. In the case of an anonymous communication, the address of the originating PUA needs to be dynamically changed for each session. When a dynamic temporary address is used for anonymous communications, a record of the mapping between dynamic address and static address should be maintained SA - Determines how best to provide anonymity UCI - Supports anonymous labels

SC 1.10 Using an alias

When communicating in certain environments users may wish to assume an identity different from their real identity. An example of this would be networked role-playing game where this assumed identity may take the form of a nickname or be that of a fictional character.

System capability No SC 1.10 - Using an alias
The system should provide the option of assuming an alias.

Supports	UR 1.3 - Increasing the options available to the originator UR3.8 - Additional Information
Possible conflicts	SC 3.5 - Assuring identity
Requirements analysis	PUA - Instruct to communicate with an alias in the UCI and not the authorized "label" UCI - Supports anonymous labels

SC 1.11 Identifying the originator of communication

The identity of the originator of a communication should be available to the recipient of that communication. If the identity of the originator is withheld for whatever reason (see System Capability **SC 1.9**) then the recipient should be informed of this fact. Similarly if the originator is assuming an alias (see System Capability **SC 1.10**) this should be indicated to the recipient. Ideally the Personal User Agent should be able to capture this identity for use in an "address book" function.

The notification that an originator is using an alias identity should prevent the incidence of deception by an originator pretending to be someone who they are not.

NOTE 1: There may be a requirement for Emergency Services to be able to determine the true identity of the originator of a communication even when the originator has chosen to be anonymous or is using an alias.

NOTE 2: Indication of the originator in this case would not be verified. This could only be done by incorporating an addition level of security (see SC 1.12).

System capability No SC 1.11 - Identifying the originator of communication
The system should provide the ability for the recipient of a communication to identify the originator or to be told that the originator is withholding their name or using an alias.

Supports	UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient
Possible conflicts	None
Requirements analysis	UCI - Includes a flag indicating whether the UCI is using the authentic name, an alias or is communicating anonymously

SC 1.12 Verifying the identity of the originator/recipient

Where transactions are undertaken which are required to be auditable, such as certain financial or legally binding communications, an additional method of verifying the identity and other characteristics of the originator or recipient may be required. This may be provided by authentication processes involving pin numbers, digital certificates and encryption.

System capability No SC1.12 - Verifying the identity of the originator/recipient
The system should provide the ability to verify that the identified originator/recipient is who they purport to be and not someone using the UCI of another person.

Supports	UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR1.6 - Maintaining backward compatibility UR2.2 - Ease of use
Requirements analysis	Awaiting further security analysis

SC 1.13 Users identifying themselves

There will be many circumstances where a user possessing a UCI uses a terminal which is not uniquely allocated to them. In fact for some users this could be the norm. A typical example would be the family home where fixed line telephones would almost certainly be used by more than one person. In such cases a UCI owner may wish to identify themselves to the PUA. There will be a multitude of ways available to do this but the burden on the user should be reduced to a minimum. Biometrics offer a potential automatic process for the future but current technology like Smartcards offer a useful compromise which could avoid the need for PIN entries.

System capability No SC1.13 - Users identifying themselves
The system should provide the opportunity for a user to identify themselves, using their UCI, when using any terminal.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	UR1.6 - Maintaining backward compatibility UR2.2 - Ease of use
Requirements analysis	Identification verifier - Depending on terminal and network this should enable user to use an appropriate means to identify themselves SA - Needs the capability to interrogate the user about their identity

SC 1.14 Awareness of cost implications of filtering/routing

Setting up a re-directing/filtering strategy may well have cost implications for the recipient. It is important that the recipient can determine these costs from the Personal User Agent. As an example, a user going abroad for a holiday will have a range of options varying from forwarding of all communications to directing all communications to a mailbox at the home location. Making a judgement without knowing the cost implications would be difficult. The functionality of the PUA could range from merely costing out specified strategies to actually proposing the best option from a cost point of view.

System capability No SC 1.14 - Awareness of cost implications of filtering/routing
The system should provide costing information on different re-directing/filtering configurations.

Supports	UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR2.2 - Ease of use
Requirements analysis	PUA - Requests SAs to provide tariff information

SC 1.15 User control of personal user agents

A PUA may perform activities on behalf of the user such as directory searches, maintenance of communications history, and incoming communications management. These activities may be explicitly user requested, triggered by external events according to a program specified by the user, or activities that have been initiated as a result of an analysis of the user's behaviour. In order to ensure that the Personal User Agent does not perform actions that are against the user's wishes, the user must always be in a position in which they can assume overall control and, if necessary, override any actions that the Personal User Agent is planning to take.

User requirement No SC 1.15 - User control of personal user agents
Users require ultimate control over their communication environment. This implies that users require the Personal User Agent to perform actions on their behalf only with their explicit or implicit agreement. Users should always have the ability to prevent the Personal User Agent from carrying out actions that they do not wish to happen.

Dependent on	UR1.8 - Trust in the system UR2.2 - Ease of use
Possible conflicts	UR1.8 - Trust in the system UR1.6 - Maintaining backward compatibility

7.2 System capabilities (internal/automated)

SC 2.1 User location monitoring

A Personal User Agent could employ a number of ways to monitor the location of the user. It is already possible to programme diaries into systems and to poll terminals in order to determine routing of communications. In the future this could be augmented with such things as tracking devices and AI based prediction.

System capability No SC 2.1 - User location monitoring
The system should monitor users' location to enable users' communications to be effectively managed dependant on their current location.

Supports	UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient
Possible conflicts	SC 3.1 - Provision/non-provision of location information
Requirements analysis	PUA - Follows user instructions on how location information is to be used SA - Feeding service specific information to the PUA

SC 2.2 User availability for communication

A Personal User Agent could employ a number of ways to monitor the availability of the user for communication and route calls accordingly. With GSM mobile, the network is aware that a terminal is switched on and therefore "available". Similarly chat rooms and instant messaging systems on the Internet presuppose that the user has registered "availability".

System capability No SC 2.2 - User availability for communication
The system should monitor users' availability to enable users' communications to be managed dependant on their current availability.

Supports	UR 1.4 - Increasing the options available to the recipient
Possible conflicts	SC 3.2 - Provision/non-provision of availability information
Requirements analysis	PUA - Follows user instructions on how availability information is to be used SA - Feeding service specific information to the PUA

SC 2.3 Establishing contact where possible

Establishing contact is arguably the most important requirement of any communication system. Current systems, however, will typically attempt to establish contact once and then abandon the attempt if unsuccessful. Advanced terminals will have far more communication options available and the chances of establishing contact will increase accordingly (e.g. send an email voice note if a voice call cannot be established and a voice-mail service does not exist).

System capability No SC 2.3 - Establishing contact where possible
The system should provide, when necessary, options in order to maximize the possibilities of establishing communication (subject to any overriding requirements of the originator or recipient).

Supports	UR 1.5 - Dealing with conflicts between originator and recipient
Possible conflicts	SC 1.6 - Selecting sending communication medium and characteristics
Requirements analysis	PUA - To try alternative means of communication as determined by users profile

SC 2.4 Taking account of local time

With current communications technologies, research has shown that people establish strategies for using these technologies that acknowledge the social behaviours of the people with whom they are communicating. These social behaviours are referred to as "social protocols". An obvious example of this is that personal telephone calls made after 11.00 pm tend to be urgent ones and people receiving such calls will assume that the caller has a genuine urgent need to communicate with them. In any advanced system where responsibility for establishing a communication is handed over to a Personal User Agent, this agent must be able to determine the local time at the location of each active terminal handling real-time services.

System capability No SC 2.4 - Taking account of local time
The system should be able to determine the local time at the location of each active terminal handling real-time services.

Supports	None
Possible conflicts	SC2.3 - Establishing contact where possible
Requirements analysis	PUA - Correctly interpret user profile rules for communicating parties

SC 2.5 Using the originator's alphabet

The originator of a communication usually requires that their identity is presented in the form in which it would normally be presented on paper. If the originator uses an alphabet other than the standard Latin alphabet when their identity is written on paper, they usually wish their identity to be presented in this alphabet where the recipient of the communication is able to display that alphabet. The originator still requires their identity be displayed in cases where the recipient of the communication is unable to display the originator's alphabet.

System requirement No SC 2.5 - Using the originator's alphabet
The system should enable originators to present their identities to the recipient using the alphabet in which their identity is normally presented on paper, where the recipient has agreed to receive information in that alphabet.

Supports	
Possible conflicts	None
Requirements analysis	PUA - Determines capability of terminal and service Terminal - Provides appropriate range of characters

SC 2.6 Using the user's preferred language for network information/instructions

During communication set up, information, queries and instructions may be passed to the originator, (and less frequently to the recipient), by various elements of the system. Ideally these should be in the language preferred by the originator (or recipient).

System capability No SC 2.6 - Using the user's preferred language for network information/instructions
The system should present information and instructions from the networks to the originator and/or recipient in their preferred language wherever possible.

Supports	
Possible conflicts	
Requirements analysis	PUA - The originator's PUA will need to have access to this information and inform the SA of the preferred language for network announcements SA - The SA will need to instruct its network or service to deliver information/instructions in the language that the PUA has specified UCI - There could be an element within the additional information field which indicates the preferred language for network information and instructions. Alternatively this information could be held by the PUA and may not need to part of the UCI

SC 2.7 Establishing the communication in a mutually acceptable language

Users will prefer that, whenever possible, the communication is established in their preferred language. An example might be an email or voice call to a large multi-national company where the user can be automatically connected to a person able to communicate in the language of choice. Technical developments in the future may allow the interposition of a real-time translation process when a communication is set up between PUAs that are unable to negotiate a language acceptable to both originator and recipient.

System capability No SC 2.7 - Establishing the communication in a mutually acceptable language
Where the circumstances allow, communications should be established in the language which best meets the requirements of both the originator and the recipient.

Supports	UR 1.3 - Increasing the options available to the originator
Possible conflicts	UR 1.5 - Dealing with communications conflicts between originator and recipient
Requirements analysis	PUA - The originator's PUA will aware of the originator's language preferences and the recipient's PUA will be aware of the recipient's capabilities. Initial negotiation will determine a mutually acceptable language if available UCI - basic language information should be stored in the additional information field of a UCI. When a UCI is stored in an address book this would give immediate indication (when selecting an address) that the selected user only understands a particular language

SC 2.8 Barring/enabling incoming communications from specified originators

A basic user requirement in any communication system is that the called user is able to bar unsolicited/unwanted calls or communications. This is a particular problem in current email services, but it is also becoming so in traditional telephone communication.

Current approaches to solve this problem have different degrees of success. For telephony there are supplementary services that prevent a calling party reaching a called party, but these are only valid for a single telephone number. Changing the telephone number from which a call is made is an easy way to override this service. For electronic mail, filtering is usually a possibility in the client software. Again, a procedure as easy as changing an email address may easily override the filter and reach the recipient.

The availability of a certified identification scheme would allow the called party to instigate a blacklist, i.e. a list of the identifiers from which they do not wish to receive communications of any kind.

An interesting approach to avoid "spam" (unwanted emails) has been suggested in some user surveys (e.g., 6th GVU WWW User Survey): an opt-out system, where a registry would contain the addresses of people who do not wish to receive mass emailings (c.f. Telephone Preference Services and Malicious Calls Bureau).

System capability No SC 2.8 - Barring/enabling incoming communications from specified originators
The system should provide the ability to bar communications from selected originators or to allow communications from selected originators.

Supports	UR1.4 - Increasing options available to the recipient SC1.2 - Editing the communication configuration
Possible conflicts	UR2.2 - Ease of use SC2.3 - Establishing contact where possible
Requirements analysis	PUA - Implementation of supplementary service like capabilities

SC 2.9 Maintaining the functionality of network-specific services

Currently, individual networks offer a large range of supplementary and other services specific to that network. Any future network architecture should enable users to have continued access to that functionality. In many cases this will not be a problem; the new architecture will automatically enhance an existing service. For instance, access to the UCI name label will be a much more effective identifier of the originator than Calling Line Identity (CLI). But even in this case, see UR1.6, it will be necessary to ensure that users with CLI enabled displays will still receive any CLI information sent. In other cases, services may need to be specifically provided to replicate the single network services they replace. An example of this might be conference calls.

System capability No SC 2.9 - Maintaining the functionality of network specific services
A UCI based system will not render inaccessible the functionality available with an existing network.

Supports	UR1.6 - Maintaining backward compatibility
Possible conflicts	UR2.2 - Ease of use
Requirements analysis	PUA - When invoking particular actions, no unexpected actions should occur SA - When invoking particular actions, no unexpected actions should occur

7.3 Service capabilities relating to UCI security

SC 3.1 Provision/non-provision of location information

A feature of evolving communications services is the ability of the system to know the geographical as well as the virtual location of the user.

In some situations it is required to know the location of a caller, for example emergency call services. Some services may not operate without such data, for example "find me the nearest hamburger restaurant". The resolution required by such systems may be established by regulation (emergency calls) or by market need (the hamburger example) and the degree of conformance may be limited by the technology (a few wavelengths in radio, a residence in fixed lines).

Other than in cases where location data is a mandate for the requested service to operate (either by regulation or by the service definition itself) the user should be able to restrict the availability of location data. On initial registration to the PUA location information may be required to allow appropriate identification of network resources.

Categories for which different levels of availability of location information may be required include:

- other persons;
- selected services, persons;
- system services (billing, etc.);
- emergency services.

System capability No SC 3.1a - Providing location information
The system should provide the option of allowing others to determine a user's physical geographical location when this information is available.

System capability No SC 3.1b - Not providing location information
The system should provide the option of not allowing others to determine a user's physical geographical location when this information is available.

Supports	UR1.9 - User control of personal user agents UR1.10 - Trust in the system
Possible conflicts	SC 2.1 - User location monitoring
Requirements analysis	Registration of user to PUA has to be able to pass location data which may be used in turn to select a local SA for each service. PUA has to be able to select appropriate SA for location of user. May need to mask SA location data which suggests that all system elements may need to use and suppress such information. The provision of charging information to the originator of a communication should not provide clues to the location of the recipient.

SC 3.2 Provision/non-provision of availability information

Instant messaging systems such as AOL's Buddy List are good examples of what is, in effect, a relatively unsophisticated PUA currently in common use. Most systems of this type work to the default that unless the user indicates otherwise he or she will be accessible by anybody else who subscribes to the service.

Users have differing requirements for privacy.

A filtering process can be used exclude unwanted communications or only allow specific ones. It should be possible to provide an ex-directory function making a user's personal identity unavailable from any directory search.

The increased capability of the system would mean that the user could specify a more precise and selective form of privacy than can be currently achieved.

System capability No SC 3.2a - Provision of availability information
The system should provide the option of allowing others to determine whether a user is available for communication.

System capability No SC 3.2b - Non-provision of availability information
The system should provide the option of not allowing others to determine whether a user is available for communication.

Supports	UR 1.9 - User control of personal user agents UR1.10 - Trust in the system
Possible conflicts	SC2.3 - Establishing contact where possible
Requirements analysis	Registration of user to PUA has to be able to pass availability data which may be used in turn to select a local SA for each service. PUA has to be able to select appropriate SA for location of user.

SC 3.3 Providing confidentiality/privacy of stored data

The communications network architecture necessary to support all the requirements of the present document will, of necessity, require that personal data on users is stored and transmitted. A typical example would be directory search data which could be stored centrally and accessed by a large number of search engines or PUAs. In such cases although a user may find it acceptable for a UCI to be determined by input of their address or date of birth, they would not want this sort of information made available to a third party (unless, perhaps, it was a close friend). A privacy policy would enhance users' trust in the system. Such a policy could prescribe that it is ultimately for users' to decide who has access to what personal data.

Service capability No SC 3.3 - Providing confidentiality/privacy of stored personal data
The system should provide assurance that stored personal data will not be accessible other than in a manner determined by the user and managed on their behalf in accordance with appropriate regulations.

When legislation demands, it must be possible for authorized persons (police etc) to monitor part of the communication e.g. to prevent terrorism, drug dealing, etc.

Supports	UR1.10 - Trust in the system
Possible conflicts	UR 1.9 - User control of personal user agents SC 1.1 - Providing communication configuration status SC 1.2 - Editing the communication configuration SC 1.5 - Determining a UCI (if unknown) by means of a search process
Requirements analysis	Covered by the UCI security analysis (see clause 13)

SC 3.4 Providing confidentiality/privacy of communications

Users require that their communication is not likely to be read or overheard by a third party or parties either intentionally or unintentionally.

Service capability No SC3.4 - Providing confidentiality/privacy
The system should provide assurance that users' communications (of speech, video or data in any format) will not be read other than by the intended recipient.

Supports	UR 1.10 - Trust in the system
Possible conflicts	None
Requirements analysis	The PUA should only specify communication options where such confidentiality/privacy can be assured. Also covered by the UCI security analysis (see clause 13)

SC 3.5 Assuring identity

One of the most important functions of an identification system is that someone who encounters the identifier can trust that the person or entity described by the identifier is the person or entity to whom the identifier belongs. The degree to which the identity described in the identifier matches the identity of the person using the UCI will be dependant on the rigour of the registration process between the user and the PUA corresponding to the UCI.

The trust needs to be of a sufficient level to satisfy users that they can safely undertake the majority of communications transactions. Where very high-risk transactions are undertaken, such as certain financial or legally binding communications, an additional method of verifying the identity and other characteristics of the party may be required (which may or may not involve the UCI) (see SC 1.12).

The identity of the originator of a communication should be available to the *recipient* of that communication. If the identity of the originator is withheld for whatever reason (see SC 1.9) then the *recipient* should be informed of this fact. Similarly if the originator is assuming an alias (see SC1.10) this should be indicated to the *recipient*. Ideally the Personal User Agent should be able to capture this identity for use in an "address book" function.

The notification that a caller is using an alias identity should prevent the incidence of deception by an originator pretending to be someone who they are not.

NOTE: There may be a requirement for Emergency Services to be able to determine the true identity of the originator of a communication even when the originator has chosen to be anonymous or is using an alias.

System capability No SC 3.5 - Assuring identity
The system should provide the ability to unambiguously identify the originator/recipient of a communication or, in the case of a recipient, to be told when the originator is withholding their name or using an alias.

Supports	UR 1.10 - Trust in the system SC 3.7 - Providing accountability
Possible conflicts	SC1.9 - Providing originator anonymity SC1.10 - Using an alias
Requirements analysis	Covered by the UCI security analysis (see clause 13)

SC 3.6 Providing integrity

When email or other data travels across the Internet, it routes through various gateways. Users need to trust that any such data has not been altered.

Service capability No SC3.6 - Providing integrity
The system should provide assurance that the communication received by the recipient shall be the same as the one that was sent by the originator

Supports	UR1.10 - Trust in the system SC 3.7 - Providing accountability
Possible conflicts	None
Requirements analysis	Covered by the UCI security analysis (see clause 13)

SC 3.7 Providing a non-repudiation capability

The provision of a non-repudiation capability is a specialist requirement of a communication system which is essentially concerned with the capability of auditing transactions. The provision of a non-repudiation capability avoids a situation where one party in a communication can deny participating in the transaction/communication or can dispute the claimed content of a transaction/communication. To provide accountability the system must:

a) be capable of proving who were the participants in the communication; and

b) prove that the data received during the communication was identical to the data sent.

Thus the system must possess be capable of verifying identity and must posses integrity.

Service capability No SC 3.7 - Providing a non-repudiation capability
The system should be capable of providing assurance that transactions undertaken as part of a communication are auditable and cannot be disowned.

Supports	UR 1.10 - Trust in the system
Possible conflicts	SC1.9 - Providing originator anonymity SC1.10 - Using an alias
Requirements analysis	Covered by the UCI security analysis (see clause 13)

7.4 System capabilities relating to the UCI

SC 4.1 Delivery (and possible processing) of a user friendly label to the recipient's PUA and terminal

The originator will need to be able to define whether an authentic label or an alias is to be sent to the recipient or if the communication is to be anonymous. In addition, it may be appropriate to have several authentic variants of their name. For instance, it may be appropriate to refer to oneself as Mr J Smith in a formal context or John Smith in a less formal communication. Both could be authenticated names. This label must be delivered by the system from the originating PUA to the recipient PUA. The recipient PUA will then be responsible for the delivery of the label to the recipient's terminal.

The recipient will wish to know which part of the label is a company name which is a family name and which is a given name. For instance the label "John Smith Andrew Martin" could be read in a variety of orders but is meant to be Martin Andrew from the brewery Company John Smith. Order of presentation is not consistent across culture and so may not be capable of standardization. An indication of order may be necessary in the addition information field.

Under normal circumstances the label will merely be delivered at the recipient's terminal, all routing and filtering will be carried out on the numeric part of the UCI. In some circumstances however when an expected communication comes from an unknown UCI but a known label it may be necessary to have the capability to process the label as well. An example would be where a communication is expected from somebody I met at a conference by the name of Fred Briggs: he did not have his UCI handy but obviously I got his name. I instruct my PUA to accept a call from somebody with a "Fred Briggs" label whatever the number.

Service capability No SC 4.1 - Delivery of a user friendly label at the recipient's terminal
The system should be capable of "transporting" the UCI label and displaying it to the recipient of a communication.

Supports	UR 1.8 - Provision of a Universal Communications Identifier
Possible conflicts	SC 1.9 - Providing originator anonymity SC 1.10 - Using an alias
Requirements analysis	PUA - Delivery, and storage of, the maximum length of UCI label to the receiving terminal using appropriate method Terminal - Capable of outputting and storage (optional) of the maximum length of the UCI label to the recipient

SC 4.2 Delivery and interpretation of a numeric part of UCI

The numeric part of the UCI is the part that is processed with the UCI-based system to determine the location of the associated PUA. The numeric part of the UCI is assigned to the UCI owner by an assignment body according to the number assignment rules that apply to the country in which the UCI owner makes their application. The same numeric part of the UCI may be associated with more than one of the UCI owner's UCI labels.

The numeric part of the UCI may be entered into any communication terminal to enable the UCI owner to be reached.

Service capability No SC 4.2 - Delivery and interpretation of a numeric part of UCI
The system should be capable of delivering and the numeric part of the UCI and using it for routing.

Supports	UR 1.8 - Provision of a Universal Communications Identifier
Possible conflicts	None
Requirements analysis	PUA and/or SA - Delivery and storage of the maximum length of UCI number to the receiving terminal using appropriate method. PUA - When a dynamic temporary address is used for anonymous communications, a record of the mapping between dynamic address and static address should be maintained. (Optionally)Terminal - Capable of storing and outputting the maximum length of the UCI number to the recipient

SC 4.3 Delivery and processing of additional information to the recipient's terminal

System Capability SC 2.8 suggests that communications can be routed/filtered dependent properties of the originator (e.g. Business or private) and System Capability SC 3.5 requires that a recipient should know when an incoming communication is from an aliased or anonymous originator. These and other requirements will require the inclusion of appropriate data/flags embedded in the UCI. It follows therefore that a user identifier should contain extra authentic and trustworthy information about the originator on which the recipient can base decisions on acceptance and/or routing.

The additional information field needs to contain information which is permanent and will be of use locally by anybody receiving and storing it. Hence it would not be appropriate to flag the urgency of a communication in this field since this applies only to a specific communication. The field should remain flexible: inevitably there will be new service capabilities in the future which may require to be catered for as a flag in the additional information field. Current thinking is that the capability to include the following information is required.

- This UCI has an authentic, registered label.
- This UCI has an unauthentic or an alias label (could be default).
- This UCI has no label (anonymous).
- Order of presentation in label (e.g. "surname, forename, company").
- The preferred language for communications is XXXX.
- This is a private/corporate UCI.
- The preferred alphabet for communications is XXXX.
- The preferred communication mode - voice/written (this would be very appropriate for people with disabilities and young children).
- The registration authority.
- The availability of digital certificate yes/no.

Service capability No SC 4.3 - Delivery and processing of additional information to the recipient's terminal
The system should be capable of decoding the flags and data in the "additional information" field and taking appropriate action.

Supports	UR 1.7 - Provision of a Universal Communications Identifier SC1.11 - Identifying the originator/recipient SC1.10 - Using an alias SC 2.5 - Use the originator's alphabet SC 2.6 - Use the originator's preferred language for network information SC 2.7 - Establish the communication in the originator's preferred language SC 3.5 - Assuring identity
Possible conflicts	None
Requirements analysis	PUA - Interpretation of additional information field and respond appropriately as defined by PUA's current communications configuration PUA and/or SA - Capable of delivering and storing all the additional information to the terminal Terminal - Capable of interpreting and storing the contents of the additional information field and outputting any relevant information to the user

8 UCI Technical Requirements

The complete list of technical requirements is displayed in tables 1 to 5. Using the codes in the references column in tables 1 to 5, it is possible to trace any technical requirement back to a System Capability (as described in clause 7) and vice versa. Where it is clear that the delivery of a requirement is dependant on most elements of the UCI system, the analysis is not documented.

Table 1: PUA Technical Requirements List

No	Technical Requirements of PUAs	Ref
1	A PUA should be capable of providing user configuration information in a form which can delivered on a wide range of terminals (e.g. web interface or speech interface)	SC 1.1
2	A PUA should be capable of editing user configuration information. The amount of editing that can be done may vary according to the terminal type (e.g. full editing only from a web interface)	SC 1.2
3	The PUA should be the repository for the user's communications history across all services	SC 1.3
4	The PUA should be capable of continuously compiling a list of UCIs derived from incoming and outgoing communications plus search results. It should be able to synchronize with other terminals and applications belonging to the same user and with other associated PUAs	SC 1.4
5	The PUA should be able to initiate a search and receive results relating to an unknown UCI from a directory service, or other PUA Service Providers	SC 1.5
6	The PUA may assume a default communications medium and characteristics based on the type of terminal contacting it or may be instructed to set up a communication in a different medium	SC 1.6
7	The PUA must be capable of accepting instructions from the user via the same or different channel to the required communications channel	SC 1.6
8	The PUA should be capable of interrogation of SAs to determine tariff costs	SC 1.7

No	Technical Requirements of PUAs	Ref
9	The originating PUA must be capable of communicating the priority of communication to receiving PUA	SC 1.8
10	The originating PUA can be instructed to communicate anonymously with a receiving PUA when so required	SC 1.9
11	The PUA should be capable of being instructed to communicate with an alias in the UCI label field and not the authorized "label"	SC 1.10
12	The PUA should be able to request SAs to provide tariff information	SC 1.7 SC 1.14
13	The PUA should follow user instructions on how location/presence information is to be used	SC 2.1
14	The PUA should follow user instructions on how availability information is to be used	SC 2.2
15	The PUA should be capable of trying alternative means of communication as determined by users profile	SC 2.3
16	The PUA should be able to determine the local time at the location of each active terminal handling real-time services	SC 2.4
17	The PUA should be able to determine the alphabetic display capability of the terminals for which communications are sent or received.	SC 2.5
18	The originator's PUA should inform the SA of the preferred language for network announcements	SC 2.6
19	The originator's PUA should be aware of the originator's language preferences and the recipient's PUA should be aware of the recipient's capabilities. Initial negotiation will determine a mutually acceptable language for interpersonal communication if available	SC 2.7
20	The receiving PUA should provide the ability to bar communications from selected originators or to allow communications from selected originators	SC 2.8
21	Using a PUA will not render inaccessible the functionality available with an existing network such as supplementary services. There should be no unexpected interactions between existing network services and PUA based services	SC 2.9
22	Registration of user to PUA has to be able to pass location data which may be used in turn to select a local SA for each service. PUA has to be able to select appropriate SA for location of user. May need to mask SA location data which suggest that all system elements may need to use and suppress such information. Must be programmable to release or not release location information. User as recipient may require billing transparency (i.e. to mask local versus non-local charging) to the call originator if the billing could override location masking	SC 3.1
23	Must be programmable to release or not release availability information	SC 3.2
24	A secure environment must be provided to protect stored personal data but must be programmable to release selected information. Where the personal data relates to someone other than the UCI owner, data release my be subject to regulatory control	SC 3.3
25	The PUA should be capable of selecting appropriate services with respect to the required security/confidentiality of the communication	SC 3.4
26	The PUA must be able to identify the originator or recipient at a level of security determined by the user and/or dependent on the type of communication. As part of negotiation, the originating PUA will offer a level of authentication and the recipient PUA will determine whether that is acceptable in that particular instance or whether re-authentication is required	SC 3.5
27	The PUA should be required to select appropriate services with respect to required integrity of communication	SC 3.6
28	The PUA should maintain authenticated records and/or pointers to services used. When a dynamic temporary address is used for anonymous services communications, a record of the mapping between dynamic address and static address should be maintained	SC 3.7
29	Processing the UCI Label - Delivery, and storage of, the maximum length of UCI label to the receiving terminal using appropriate method	SC 4.1
30	Processing the UCI Number - Delivery, and storage of, the maximum length of UCI number to the receiving terminal using appropriate method	SC 4.2
31	Processing the UCI Additional Information field and taking appropriate action. Subsequently, delivering and storing all the additional information to the terminal	SC 4.3

No	Technical Requirements of PUAs	Ref
32	When a dynamic temporary address is used for anonymous communications, a record of the mapping between dynamic address and static address should be maintained	SC 3.7 SC 1.9
33	The user should be provided with a mechanism (or mechanisms) for taking control of all actions performed by their PUA. This mechanism should allow the user to initiate, pause and terminate PUA activity. It should also notify the user of actions proposed by the PUA and allow the user to agree to, query, or reject these proposals	SC 1.15
34	The PUA needs the capability to interrogate the user about their identity when user verification is requested. Many services already require a password for activation	SC 1.12

Table 2: SA Technical Requirements List

No	Technical Requirements of SAs	Ref
1	When a user communicates with a non-UCI recipient, the users PUA would not actively be involved in the communication set-up. In this instance the SA must detect that the communication is directed at a UCI and set up the communication (as a proxy PUA). It will subsequently inform the originator's PUA that a communication has been made	SC 1.3
2	The SA should provide charge detail records to PUAs of resources used	SC 1.7
3	The SA should provide the possibility to assign priority to a communication and suitable reaction	SC 1.8
4	The SA should determine how best to provide anonymity	SC 1.9
5	The SA must feed service location specific information to the PUA when appropriate	SC 3.1a SC 2.1
6	The SA must feed service specific availability information to the PUA when appropriate	SC 3.2a SC 2.2
7	The SA must be able to confirm to the PUA that the service can support the required level of communications confidentiality	SC 3.4
8	The SA must maintain a database mapping service-specific addresses to PUAs	SC 3.5
9	The SA must be able to confirm to the PUA that the service can support the required level of integrity	SC 3.5
10	The SA must maintain records of inter-object transactions	SC 3.3
11	Processing the UCI Label - Delivery, and storage of, the maximum length of UCI label to the receiving terminal using an appropriate method	SC 4.1
12	Processing the UCI Number - Delivery, and storage of, the maximum length of UCI number to the receiving terminal using appropriate method	SC 4.2
13	Processing the UCI Additional Information field and taking appropriate action if necessary. Subsequently, delivering and storing all the additional information to the terminal	SC 4.3

Table 3: Terminals and end-user applications Technical Requirements List

No	Technical Requirements of Terminals & End-user Applications	Ref
1	Terminals and applications should provide support for PUA interrogation re communications configuration (e.g. function buttons and/or applications)	SC 1.1
2	Terminal and local applications should provide support for editing the communications configuration at the PUA (e.g. function buttons and/or applications)	SC 1.2
3	Terminals and local applications need to be capable of synchronizing "address books" with PUAs	SC 1.4
4	Terminals and local applications should provide an enhanced search interface where possible	SC 1.5
5	Terminals and local applications may have a default communications medium and characteristics. They may allow the user to select alternative services and characteristics overriding the default assumptions of the PUA	SC 1.6
6	Terminals and local applications should have the capability of assigning the priority of a communication(e.g. special function button)	SC 1.8
7	Terminal and applications should provide an appropriate range of characters	SC 2.5
8	Terminals and applications should be capable of outputting and storing the maximum length of the UCI label to the recipient	SC 4.1
9	Terminals and applications should be capable of storage the maximum length of the UCI number from the recipient	SC 4.2
10	Terminals and applications should be capable of interpreting, presenting and storing the contents of the additional information field	SC 4.3

Table 4: UCI Technical Requirements List

No	Technical Requirements of the UCI	Ref
1	Supports anonymous labels	SC 1.9
2	Includes a flag indicating whether the UCI is using the authentic name, an alias or is communicating anonymously	SC 1.11
3	There could be an element within the additional information field which indicates the preferred language for network information and instructions. Alternatively this information could be held by the PUA and may not need to part of the UCI	SC 2.6
4	Whether language preference information is contained in the additional information field is dependent on the emerging network architecture. In any case having basic language information in an address book embedded in UCIs could be useful to users i.e. and immediate indication when selecting an address that this UCI holder only understands a particular language. Naturally this information could be stored in other ways	SC 2.6

Table 5: Identification Verifiers Technical Requirements List

No	Technical Requirements of Identification Verifiers	Ref
1	Depending on terminal and network this should enable user to use an appropriate means to identify themselves	SC 1.13

9 UCI system dialogues, services and processes

From an analysis of the system capabilities (see clause 7) and the UCI Technical Requirements (see clause 8) it is possible to determine the need for a number of important system dialogues, support services and key processes.

9.1 System dialogues

In order to understand the key system dialogues, it is necessary to have a model of the information flow paths between the different UCI system entities. These paths are shown in table 4.

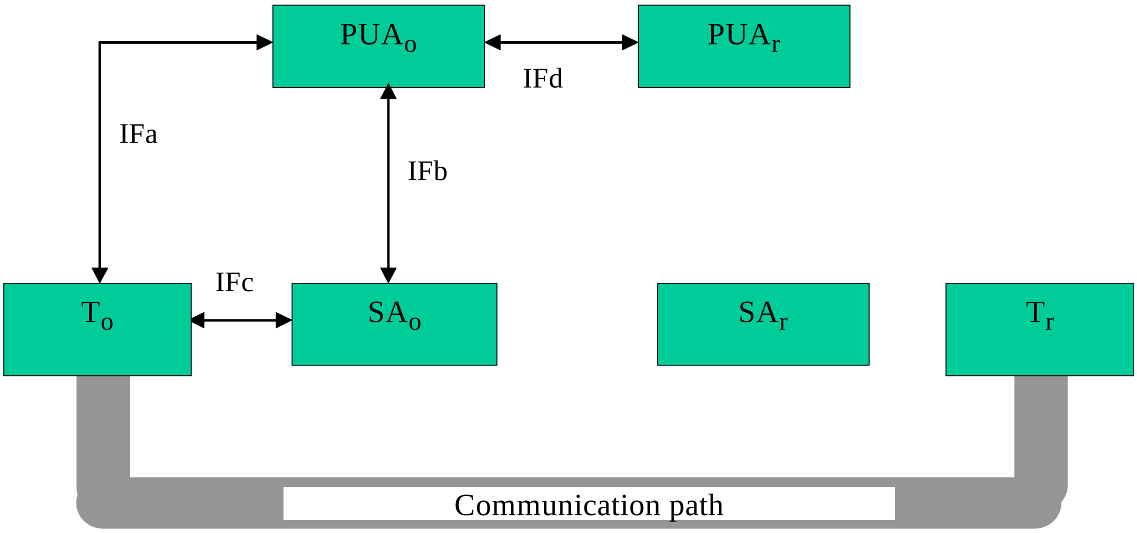


Figure 4: Information flows in UCI system dialogues

The entities shown in figure 4 are as follows:

- T_o, T_r - The communication terminal of the originator and the recipient of a communication respectively;
- PUA_o, PUA_r - The PUA of the originator and the recipient of a communication respectively;
- SA_o, SA_r - The SA of the originator and the recipient of a communication respectively.

The operation of UCI based systems to support person-to-person communication depends critically on the dialogues between the system entities identified in clause 6. The three most important dialogues are between users and their PUAs, between the PUAs of the communicating parties and, finally, the dialogue between a PUA and an SA.

- User to PUA dialogues (IFa in figure 4) - These must support:
  - the user registering themselves with the PUA (this may happen automatically for some types of network or service);
  - the user requesting a specific type of communication with another person;
  - the user managing their PUA;
  - the PUA keeping the user aware of status information and feedback.
- PUA to PUA dialogues (IFd in figure 4) - These must support a number of activities including:
  - making propositions for desired communication outcomes (e.g. "real-time standard quality voice communication required");
  - responding to communication propositions (e.g. "real-time standard quality voice communication accepted - connect to [connection point]" or "can only support real-time low quality voice communication");

  - a process of negotiation to achieve a mutually acceptable outcomes.

The "FIPA Communicative Act Library Specification" proposed by the Foundation for Intelligent Physical Agents (FIPA) is a candidate model for handling such activities.

- PUA to SA dialogues (IFb in figure 4) - These must support a number of activities including:

  - requesting the discovery of network/service/terminal capabilities;
  - requesting the establishment, management and termination of communication paths/sessions;
  - the presentation/restriction of non-UCI identities (e.g. the telephone number of the user's terminal) to the network/service

The APIs contained in ES 201 915 [13] and those being defined by 3GPP OSA, PARLAY and JAIN™ are candidate models for handling such activities.

The most crucial communication in terms of satisfying the user's communications needs is the PUA to PUA dialogue. This communication is involved in negotiating the "social protocols" between the two (or more) communicating parties. The course of these negotiations will be determined by the preferences of each of the communicating parties as captured in the settings and rules in their personal profile in their PUA. The satisfaction of the vast majority of the user requirements identified in the present document will be dependant on this PUA to PUA dialogue. The PUA to PUA dialogue is very dependant on the accuracy and content of the information upon which it is based (e.g. if the UCI is being used by someone other than the true UCI owner, this may lead to undesirable outcomes).

Annex A shows several examples of how the PUA to PUA dialogue enables satisfactory "social protocols" to be realized.

9.2 Support services

A number of support services will be needed to deliver the full capabilities of UCI and some have already been identified as part of the activities described above. Many of these services are being actively considered in other bodies in (e.g. EP TIPHON, IETF), and their need in UCI system is under consideration.

Key services already identified include:

- Resolution Service (RS)

  Provides a translation of the numeric element of any UCI to the address of its associated PUA for use in routing. This resolution service needs to be global in its scope and thus able to resolve the UCI wherever it is used.

- Signalling Routing Service (SRS)

  Provides a signalling path from:

  - PUAs to PUAs, based on routing addresses provided by the Resolution Service;
  - UCI owners' terminals to their PUAs;
  - PUAs to SAs.

- Discovery Services - e.g. to enable the PUA to determine the current terminal capabilities of the user's terminal.
- Presence/Availability Services - e.g. to enable the PUA to determine whether the user is able and willing to use their terminal.
- Location Determination Service (if this is not part of Presence Services) - e.g. to enable the PUA to determine whether the user is in their home location or is travelling.

- Identification Services.

  These services must allow users to reliably identify themselves as the person using a communications device or application. They could use a physical device such as a Smart Card Reader into which they can put their UCI-based identification card, or could use identification information on a Subscriber Identity Module (SIM) or a UMTS_Subscriber Identity Module (USIM) in a mobile phone, or could be a process of logging into an application with a username or password.

9.3 Key processes

To fully describe the operation of UCI-based systems, a number of processes need to be described. These processes include registration, profile modification, outgoing and incoming communication. Automatic terminal registration, following the example of GSM, and service registration are seen as pre-requisites for the most successful implementation of a UCI service - although manual registration methods will also be examined to ensure that registration is a possibility in even the most inhospitable communication environments. Some of these key processes are described in the following clauses.

9.3.1 Terminal/User registration and authentication

During terminal registration, attach requests are sent from the terminal via the network attachment point through to the PUA. Location registration data collected by the selected SA is passed to the PUA to update the User profile.

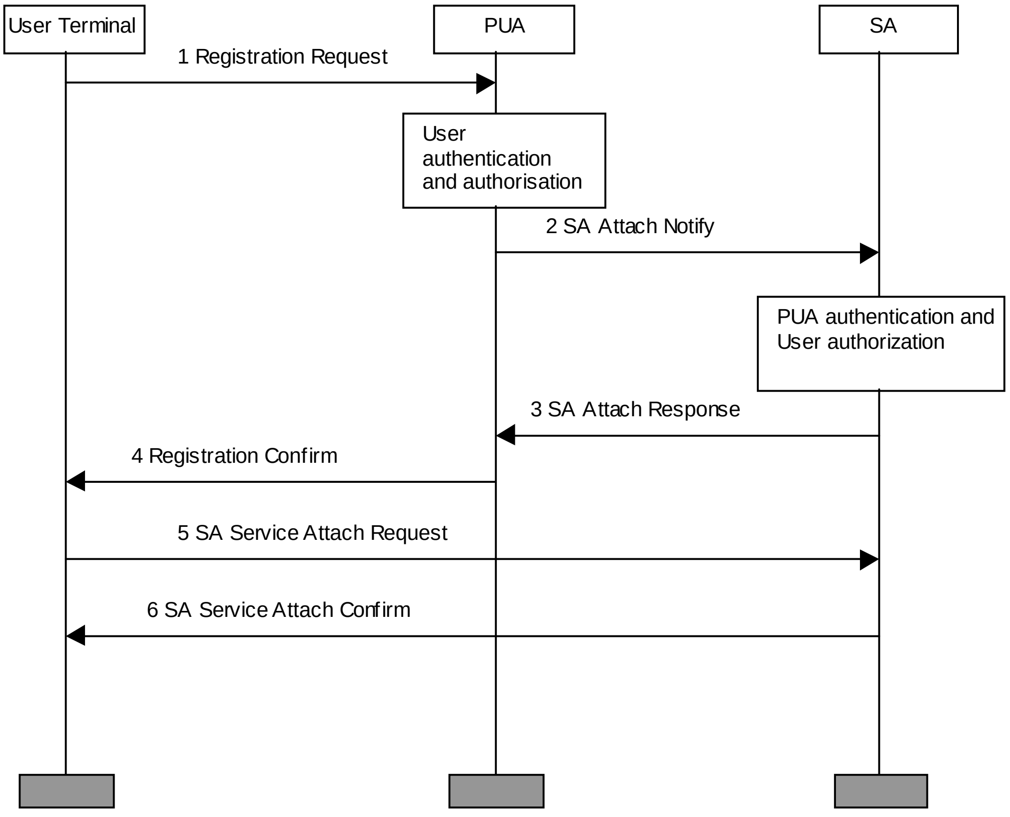

User Terminal
PUA
SA
1 Registration Request
User authentication and authorisation
2 SA Attach Notify
PUA authentication and User authorization
3 SA Attach Response
4 Registration Confirm
5 SA Service Attach Request
6 SA Service Attach Confirm

Figure 5: Information flows for terminal/user registration and authentication

The PUA/SA bind (establishment of a mutually agreed association) then allows the SA to continuously inform the PUA about changes that take place with respect to the user's terminal/communication status (e.g. when a call is terminated, the SA will inform the PUA so that the PUA can update its communication records).

Where a PUA has a binding with another PUA (e.g. club scenario situations) the slave PUA must inform the master of changes.

The flows shown in figure 5 are described in more detail in table 6:

Table 6: Description of flows for terminal/user registration and authentication

Message Number	Message Description
1	A user stimulus (e.g. turning on the terminal to get service) sends a message containing (at least) the required service(s), an Authentication Token and a UCI Private Identity
	The AuthenticationToken is used to authenticate the user. The offered UCI Private Identity is checked to ensure that it matches to User-Profile. The service(s) are also checked to see if the user is authorized to use such service(s). If no User-Profile or service(s) exist for the offered UCI Private Identity then the PUA will reject the registration attempt
2	A message is sent to the SA relevant to the requested service(s) containing the UCI of the user, the PUA Private Identity, the Service(s) to be supported, and a ticket to allow validation of the request. If the request is rejected alternative SAs may be tried. If all attempts are rejected the PUA will send a rejection message back to the user
	The SA checks the PUA's certificate and verifies that it has sufficient resource to fulfil any requests from the client against the service invoked
3	A message is sent to the PUA with an authorization ticket valid for the requested service(s)
4	The PUA composes and sends the service credentials (ticket) to be sent to the user
5	The user (terminal) creates a message to send to the SA based upon the content of the service credentials supplied by the PUA
6	The SA validates the ticket sent from the user and, if correct, offers service and confirms this with the SA Service Attach Confirm message
NOTE: In some cases, such as fixed telephony networks, registration and authentication is implicitly achieved at the time of service provision.	

9.3.2 Basic UCI communication set-up

UCI communications are achieved by means of a negotiation process between the originating and recipient sides of the communication based upon the user preference rules and service capabilities that are stored in the originating and recipient PUAs. The negotiation process is also based upon obtaining an accurate assessment of the current capabilities of the originating and recipient users and a consideration of the security and privacy of data used in the negotiation.

The SA_o and SA_r assist the originating and recipient networks respectively for communication set-up. The information flows describe the signalling messages flowing between the entities (SA, PUA) needed to assist the underlying networks to set-up the communication.

Prerequisites for a basic UCI communication are:

1) The UCI recipient is registered with at least one SA for the requested services.

2) The UCI profile stored in the PUA maintains the transport address and the logical address of the Service Agent (SA) corresponding to the services registered for the UCI User.

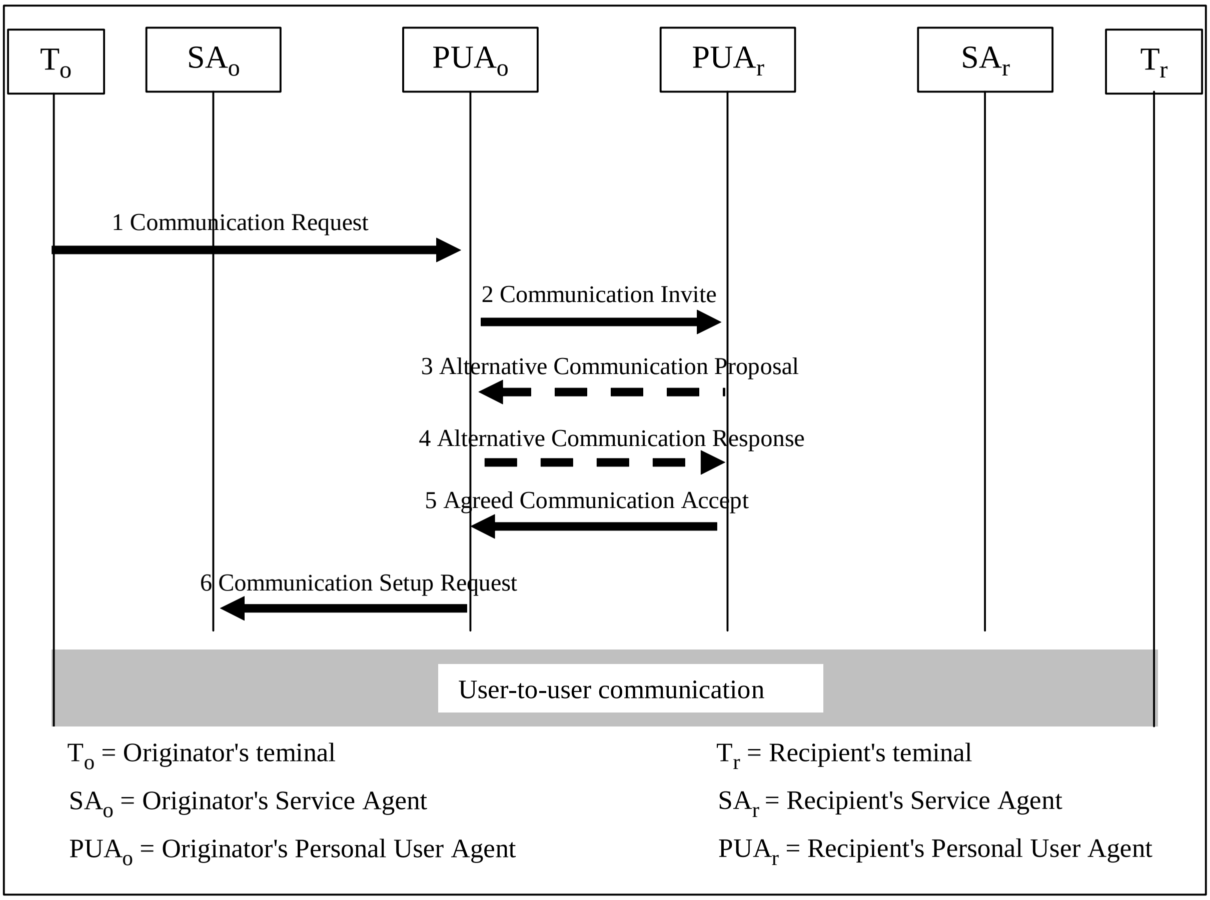

T_o
SA_o
PUA_o
PUA_r
SA_r
T_r
1 Communication Request
2 Communication Invite
3 Alternative Communication Proposal
4 Alternative Communication Response
5 Agreed Communication Accept
6 Communication Setup Request
User-to-user communication
T_o = Originator's teminal
SA_o = Originator's Service Agent
PUA_o = Originator's Personal User Agent
T_r = Recipient's teminal
SA_r = Recipient's Service Agent
PUA_r = Recipient's Personal User Agent

Figure 6: Information flows for basic UCI communication set-up

The flows shown in figure 6 are described in more detail in table 7:

Table 7: Description of flows for basic UCI communication set-up

1	The originating user initiates the sending of a "Communication Request" from terminal (T_o) to be delivered to PUA_o
2	The PUA_o identifies that this communication is from its UCI User by checking the UCI Private Identity used for terminal/service registration. The PUA_o identifies the recipient address by inspection of the UCI_r and sends the "Communication Invite" to the Recipient's PUA (PUA_r) including a Displayable Name (CLI)= UCI_o
	If PUA_r, identifies that the request is one that it cannot accept (because of the basic capabilities of the recipient's communication environment or because of the recipient's wishes as expressed in their PUA rules, flows 3 and 4 are initiated. If the request can be met without query, the dialogue moves to flow 5
3	PUA_r rejects the initial request and sends an "Alternative Communication Proposal" - giving an indication of another potentially acceptable option
4	PUA_o proposes an "Alternative Communication Response" to PUA_r
	Flows 3 and 4 are repeated until PUA_r is able and willing to accept the communication
5	PUA_r identifies the service type from the "Communication Invite" (or "Alternative Communication Response") and determines, from information stored in PUA_r which SA to use. PUA_r sends the "Agreed Communication Accept" with destination address details for the nominated terminal (e.g. IM address, E.164 number, or SA_r address) to the PUA_o
6	PUA_o forwards the response it received from PUA_r to SA_o as a "Communication Setup Request"
	SA_o instructs it's network to set-up the communication between the two T_o and T_r

Some security issues that arise from the information flow of figure 6 are:

- The SA_r <> PUA_r binding is formed during registration and is secure.

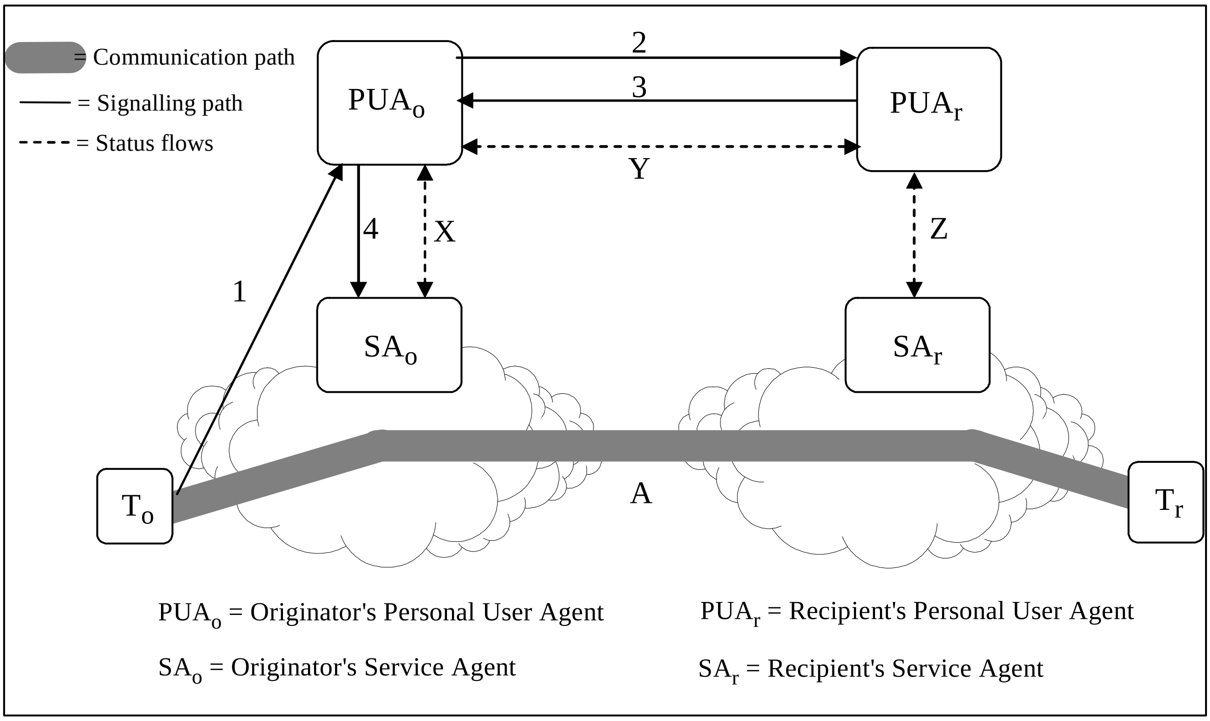
9.3.3 PUA and terminal profile management

The detailed work in this area will take place in STF199 and STF200.

10 Communication using UCIs

As people may have more than one role, there are circumstances where they may have more than one UCI and hence more than one PUA. The two examples illustrated below show the simple case of basic UCI communication (as covered in clause 9.3.2) and then an example where more than one PUA is associated with both the communicating parties. In practice, there may be circumstances that are a hybrid of these two models. Annex A shows examples that illustrate both of these models in practical every day communication situations.

10.1 PUA to PUA communication - basic



= Communication path
= Signalling path
= Status flows
PUA$_o$
PUA$_r$
2
3
Y
4
X
Z
1
SA$_o$
SA$_r$
T$_o$
A
T$_r$
PUA$_o$ = Originator's Personal User Agent
PUA$_r$ = Recipient's Personal User Agent
SA$_o$ = Originator's Service Agent
SA$_r$ = Recipient's Service Agent

Figure 7: UCI Communication Architecture for individual PUAs

Table 8: Major information flows associated with PUA negotiation

Flow	Activity
X, Y, Z	Information regarding the status of a terminal and a service may be communicated between a PUA and its SA and between PUAs before, during and after communications
1	The originator uses the UCI associated with an end user's name. This contains a digit string that is used to derive the target user's address
2	The originating PUA identifies the UCI and makes contact with the target user's PUA
3	The target user's PUA responds to the message from the PUA$_o$ by supplying necessary information to enable the communication set-up to continue. The PUA$_r$ checks that the request corresponds to an active service binding to it's user's terminal. If the original request is not fully acceptable, a negotiation with the originating PUA is needed
	Flows 2 and 3 will be repeated for each round of the negotiation until success is achieved
4	The originator's PUA supplies the SA$_o$ with the necessary information to enable the communication set-up to continue
A	SA$_o$ instructs it's network to route the communication to the terminating network based on the information supplied by PUA$_r$

The flows X, Y and Z can be used to handle a number of communication-related messages before, during and after any communication. These paths may be involved during in-session signalling between the two ends of a communication and they may also be involved in alerting the PUA at each end of the communication to a termination/clear-down of the media path for that session.

Flow Z is one mechanism whereby the underlying network or service can be instructed to deliver the UCI of the Originating user to the Target User in some form of Calling Name type service (to the extent that such services are supported by the networks/services). Where the PUA knows that the service/network associated with the Target User's SA does not support such Calling Name services, the network/service can be instructed to deliver the label element of the UCI as a message using the normal communication path (e.g. a spoken message using the speech path for a telephony communication or as a short text message where the communication path is text/graphics based).

10.2 PUA to PUA communication - linked PUAs

There are a number of cases where a second PUA may be involved on the part of the originator or the recipient of a communication or both the originator and the recipient, as shown in figure 8. A major reason for this to occur is when a person has their own UCI and also a UCI belonging to a "role" within an organization. In this case the person's own PUA will involve the "role" PUA in the establishment of communication when an outgoing communication is using the "role" UCI. Similarly, the role PUA will receive incoming communications and involve the PUA belonging to the individual associated with that "role" in order to determine how the communication should be delivered.

In multiple-PUA scenarios, a PUA may only be aware of the identity associated with the PUA with which it established direct contact and not the identity associated with any secondary PUAs. In the previous examples this will mean that users may only be aware of the identity associated with the "role" of the distant party and not the identity of the individual behind that "role".

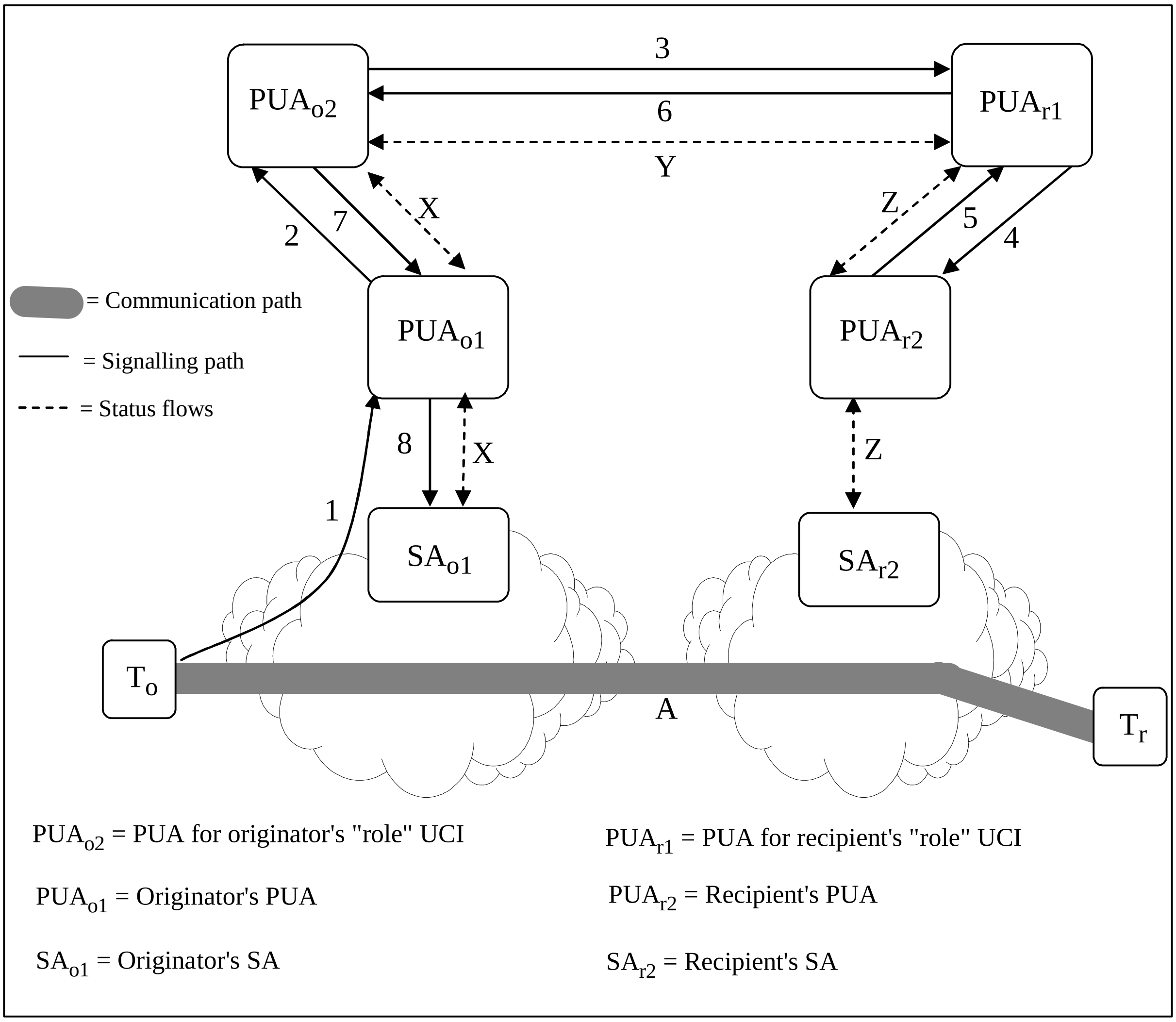

PUA$_{o2}$
PUA$_{r1}$
3
6
Y
X
Z
2
7
5
4
PUA$_{o1}$
PUA$_{r2}$
= Communication path
= Signalling path
= Status flows
8
X
Z
1
SA$_{o1}$
SA$_{r2}$
T$_o$
A
T$_r$
PUA$_{o2}$ = PUA for originator's "role" UCI
PUA$_{r1}$ = PUA for recipient's "role" UCI
PUA$_{o1}$ = Originator's PUA
PUA$_{r2}$ = Recipient's PUA
SA$_{o1}$ = Originator's SA
SA$_{r2}$ = Recipient's SA

Figure 8: UCI Communication Architecture for linked PUAs

Table 9: Major information flows for linked PUAs

Flow	Activity
X, Y, Z	Information regarding the status of a terminal and a service may be communicated between a PUA and its SA and between PUAs before, during and after communications
1	The originator uses the UCI associated with an end user's name. This contains a digit string that is used to derive the target user's address. The originator also sends a control message to his personal PUA_{o1} to involve a second PUA_{o2} (e.g. by specifying the required "role")
2	PUA_{o1} determines from the control message to involve another PUA_{o2} and makes contact with PUA_{o2}
3	PUA_{o2} identifies the UCI and makes contact with the recipient's PUA (PUA_{r1})
4	The recipient's PUA_{r1} reacts to the message from the PUA_{o2}. It determines that a second recipient PUA (PUA_{r2}) has to be involved and supplies the necessary information to enable the communication with PUA_{r2} to continue
5	PUA_{r2} responds to the message from the first PUA_{r1} by checking that the request corresponds to an active service binding to the user's terminal and returns the necessary information to enable the communication set-up to continue (or proposes an alternative communication option)
6	PUA_{r1} supplies the originating PUA (PUA_{o2}) with the necessary information to enable the communication set-up to continue (or proposes an alternative communication option)
	Flows 3 to 6 will be repeated for each round of the negotiation until success is achieved
7	PUA_{o2} supplies PUA_{o1} with the necessary information to enable the communication set-up to continue
8	PUA_{o1} supplies SA_o with the necessary information to enable the communication set-up to continue
A	SA_o instructs it's network to route the communication to the terminating network based on the information supplied by PUA_{r2}

The flows X, Y and Z can be used to handle a number of communication-related messages before, during and after any communication. These paths may be involved during in-session signalling between the two ends of a communication and they may also be involved in alerting the PUA at each end of the communication to a termination/clear-down of the media path for that session.

Flow Z is one mechanism whereby the underlying network or service can be instructed to deliver the UCI of the Originating user to the Target User in some form of Calling Name type service (to the extent that such services are supported by the networks/services). Where the PUA knows that the service/network associated with the Target User's SA does not support such Calling Name services, the network/service can be instructed to deliver the label element of the UCI as a message using the normal communication path (e.g. a spoken message using the speech path for a telephony communication or as a short text message where the communication path is text/graphics based).

10.3 UCI communication with non-UCI users

UCI requires that it should be possible for UCI users to communicate with people who have no UCIs. This implies that solutions must be found for:

1) A UCI owner establishing a communication with a non-UCI user.

2) A non-UCI owner establishing a communication with a UCI user.

Both of these options have been considered and alternative solutions that make the minimum demands on legacy systems are being derived in the work of STF199.

It should be noted that it appears that option 1) is easily achievable with a subset of the UCI-user to UCI-user communication described in clauses 9 and 10.1. Solutions based upon existing telephony network (e.g. PSTN, GSM) practices have already been considered as candidates for a solution to option 2) and their extensibility to other legacy environments is being investigated.

11 UCI Privacy Protection

11.1 Background

People who subscribe to communications services initially have almost full control of their communications privacy. Only the service supplier knows the communications identifier associated with that service (e.g. the telephone number or the email address). This means that only the service supplier has the ability to send a communication to the subscriber - but they can do so whenever they chose.

With only the service supplier knowing the subscriber's communication address nobody else will be able to contact that subscriber. Subscribers will never receive much-needed incoming communications without giving their communications addresses to others. However, in conventional communications systems, once subscribers have given their communication addresses to other people, they have lost all control over how those people may contact them.

There are at least 3 ways in which most people enable others to communicate with them:

1) Giving their communications address to specific people who they want to be able to reach them. Exchanging business cards is an example of a way to give communication addresses to others. Once a business card has been given to someone that person may contact the card owner whenever they want. Giving away a business card gives the person receiving the card the ability to contact the owner using any of the means listed on the card.

2) Attaching a communication address to individual communications. Calling Line Identity and "From" addresses on emails are examples of such attachments. Whereas per-call restriction of CLI is an available mechanism to prevent the called party having access to the identity of the calling party, most email accounts reveal the senders email address to everyone they contact (in the "From" field). The only way to avoid giving people rights of access resulting from the identity revealed in the "From" field is not to email anyone or to edit the "From" field information when sending some emails!

3) The listing of communication addresses in public directories. A person here has no control of the release of their communication address other than by deciding whether they allow it to be listed or not. Once listed, there are few ways of adding further restrictions to determine who sees and uses the identity and those that exist are usually very inflexible.

Currently the only way for people to manage receipt of communications from other people who have their communication identifier is to use some form of management service (e.g. currently specified supplementary services including selective call barring or selective call diversion or an application specific service such as email filtering). The person can easily avoid such mechanisms by using an alternative identity (e.g. an alternative telephone or a different email address).

11.2 UCI-based privacy control

Throughout the evolution of the design of a UCI based architecture, the issue of giving users maximum control of their privacy has been a key aim and is reflected in a number of the User Requirements (see annex B). The elements of the UCI architecture that contribute to giving users fine-grain control over their privacy are:

- User identification - The UCI itself gives a reliable identification of a person (or role). This identification forms the basis upon which the control of what people (or roles) get to see what information (information privacy) or get to have various rights of access to a UCI owner (communication privacy) is based. Most other identification systems do not clearly identify people, but identify terminals or service subscriptions.

- User control - The PUA contains rules that the user can modify in order to give very fine-grain control over their information and communication privacy.

- Information location - A principle that has been applied throughout the design of the UCI architecture is to ensure that, as far as possible, information is stored where it is used and it is not copied into other entities that may have lower security than the environment in which the information is used.

- Information distribution - In the design of the information flows, care has been taken to ensure that only that information necessary to achieve an outcome is passed to the entity responsible for achieving that outcome. This minimizes the danger that information is sent to entities whose Privacy Policy may not guarantee the privacy required by the user.

- UCI search - Users would have the option of allowing their UCI to be found in any UCI search. There are at least 2 options of how such searches could be supported are:

  - "Classic" directory mechanism - Here the options available to the UCI owner are whether to allow their UCI to be listed in the directory or not. It is hoped that, as the UCI gives the user much greater control over their incoming communications, more people will allow their identifier to be listed than at present (e.g. with telephone directories).

  - Some form of peer-to-peer mechanism between PUAs (where the search request is propagated to all PUAs or to PUA Providers) - In this case there is the possibility of having PUA rules related to searches. These rules could allow UCIs to be unconditionally released to people in the UCI owner's address book, and prevent release to those people on a "blacklist" within the PUA. A further level of subtlety would be where the enquirer is asked to leave a "virtual calling card" (see clause A.3.3.3).

    In practice there may be several variants and hybrids of the above two search options.

The scenarios in annex A provide several examples of the application of these principles.

A comparison of the privacy control between UCI and ENUM appears in annex F.

The degree of control of privacy is dependant upon the security of all elements of the UCI architecture. The security analysis of the UCI architecture is discussed in clause 13, with the risk assessments shown in annex E.

12 UCI Data

The operation of UCI-based systems depend on the processing of data relating to:

- the UCI owner;

- the networks, services and applications to which the UCI owner subscribes;

- the rules, expressing the user's communication preferences, that control the operation of the PUA.

Much of the data is used in processes within the entities where the data is stored. These internal processes are not the subject of description within the present document. The data is also used as the parameters passed between the different entities in UCI systems, and the information flows shown throughout the present document indicate where the communication of this data takes place.

12.1 Stored data

The storage and distribution of data is largely handled by 4 entities:

- terminals;

- PUAs;

- SAs;

- the services.

Tables relating to each of these entities follow. These tables show the information that needs to be stored by each of the entities in order that the entity has the information that is either needed to perform its own internal processes (e.g. information that a PUA needs to evaluate its stored rules) or information that is needed to pass messages to other entities (e.g. a terminal must store its own private identity to enable it to sent this data to a PUA for authentication and authorization).

Each table shows the ideal range of data that needs to be stored for each entity. Where the entity is unable to store the data shown in the tables, a process may be required to compensate (e.g. basic PSTN telephones will not have a stored UCI Private Identity and hence a separate authentication and authorization process will be needed to identify the UCI owner).

12.1.1 Terminal Data

Table 10: Terminal data

Data Description	Owner of Data	Number	Sub-elements	Public/Private	R/W	If read?	If altered?	Examples	Notes	Passed to
UCI Private Identity	Service Supplier	1		Private	R	Masquerade	Lose link to PUA	IMSI, IP Address, MAC Address, UCI Private ID on Smart Card	May not exist in PSTN except via Smart Card inserted in terminal	Own PUA
Contact's UCI	Contact	N (1 per contact)	Numeric, Label, some additional elements	Public	R/W	User's contacts identified	User's contact database corrupted. May be corrected on synchronization or may corrupt master contact database.	-	If own PUA is involved in the setup of all communications less additional elements will be needed. May be tagged or organized by "role" in which they were captured.	Own PUA

12.1.2 PUA Data

Table 11: PUA data

Data Description	Owner of Data	Number	Sub-elements	Public/Private	R/W	If read?	If altered?	Notes	Passed to
PUA Private Identity	PUA Provider	1	-	Private	R	Masquerading	All communication destroyed	-	SA
UCI Public Identity	UCI Owner	1	Numeric, a choice of Labels (some authentic the others "aliases"), and all additional elements.	Public	R	PUA owner identified	Masquerading	The public identity of the PUA.	SAs, PUAs, Terminals
Service-specific identifier	UCI Owner	N (1 per service)	-	Private	R	All of the owner's services can be identified.	This will break communication with the supplier's service (if needed to reach supplier's service).	This forms the list of all services subscribed to.	SA
Private Service Identity	Service Supplier	N (1 per service)	-	Private	R/W	Enables a communication to be made only if the service supplier is known and the PUA identity can be faked. Limited to validity period of Private Service Identity.	Can prevent communication with a supplier's service.	Can only be used by the Service Supplier to establish communications with the UCI owner (i.e. not a publicly valid address).	SA
Global Rules	UCI Owner	1 set	-	Private	R/W	The owner's communication patterns and preferences can be determined.	The operation of all services can be interfered with.	-	Possibly to SA if PUA not involved in basic communications.
Service-specific rules	UCI Owner	N sets (1 per service)	-		R/W	The owner's communication patterns and preferences can be determined	The operation of a service can be interfered with.	-	Possibly to SA if PUA not involved in basic communications.

Data Description	Owner of Data	Number	Sub-elements	Public/Private	R/W	If read?	If altered?	Notes	Passed to
UCI	Contact	N (1 per contact)	Numeric, Label, some additional elements		R/W	User's contacts identified	User's contact database corrupted. Will propagate corruption to all other contact databases on synchronization.	If own PUA is involved in the setup of all communications less additional elements will be needed. May be tagged or organized by "role" in which they were captured.	PUAs and Terminal

12.1.3 SA Data

Table 12: SA data

Data Description	Owner of Data	Number	Sub-elements	Public/Private	R/W	If read?	If altered?	Notes	Passed to
Private SA Identity	Service Supplier	1	-	Private	R	Reader could masquerade as an SA and have privileged access to PUA.	SA could be rendered inoperative. Service to many users could be disrupted.		PUA
Private Service Identity	Service Supplier	N (1 per attached subscriber that has a UCI)	-	Private	R	The reader could initiate communication if he also had access to the PUA private identity.	Prevents all communication with a user of that service.	May be loaded from the service's database and stored when user attaches to the relevant Service Point of Attachment.	PUA, SA and the Service
Public Service Identity	Service Supplier	N (1 per attached subscriber that has a UCI)		Public	R	A user's service identity is identified and may be linked to their UCI if that has also been determined	Unlikely to be a problem as the SA is unlikely to be the master database.	There is a 1:1 mapping between this and the Private Service Identifier. Loaded as above.	The service itself
Global Rules	UCI Owner	Up to 1 set per attached subscriber that has a UCI	-	Private	R/W	As for PUA	As for PUA	-	Not passed
Service-specific rules	UCI Owner	Up to 1 set per attached subscriber that has a UCI	-	Private	R/W	As for PUA	As for PUA	-	Not passed

12.1.4 Service Data

Table 13: Service data

Data Description	Owner of Data	Number	Sub-elements	Public/Private	R/W	If read?	If altered?	Notes	Passed to
Private Service Identity	Service Supplier	N (1 per service subscriber that has a UCI)	-	Private	R	Can only be used during the lifetime of the identifier if the Service Agent private identity is known.	Will prevent communication for the lifetime of the identifier.	Is recognized by the service (may need to interrogate the service Home Environment).	SA
Public Service Identity	Service Supplier			Public	R	A user's service identifier is known, but this is not easily linkable to their UCI.	A major disaster. Can be used to misroute communication.	There is a 1:1 mapping between this and the Private Service Identifier.	Service elements

12.1.5 User provided UCI data

The UCI owner is responsible for adding personal information to their PUA. The core set of data necessary for the operation of UCI systems is one or both of:

- **Authentic label data**: this data is provided by the UCI owner and verified by an Identity Authorization Authority. There may be one or more variants of the authentic label data. This data is associated with the numeric and additional information.

- **User provided label data**: this data is provided by the UCI owner and requires no third-party verification. There may be one or more variants of the user provided label data.

Where there is more than one variant of an authentic or user provided label, the version that is used in any particular communication (and hence the identity that the UCI owner conveys to the person with whom they are communicating) may depend on the context of that communication (e.g. who is trying to contact the UCI owner or who the UCI owner is trying to contact). The user may provide additional personal information. The handling of this additional information will be dependent on PUA rules provided by the user.

12.2 Acquisition of network, service and application data

Data about the status of the various networks, services and applications to which the UCI owner subscribes is critical to the operation of UCI systems. It is this data that is used to ensure that communications use network, services and applications that are fully operational and that satisfy the specific needs of the UCI owner.

In order to ensure that PUAs do not have to adopt different information interchange solutions for every conceivable communication technology, there is a requirement for standardized interfaces and protocols between PUAs and SAs.

Two different categories of information exchange between PUAs and SAs are:

- communication about establishing and managing individual end-to-end communications;

- communication about changes to the status of the user's service (e.g. whether the service is currently operational or whether the maximum achievable QoS has changed) irrespective of whether the service is being actively used for communication.

As these two categories of information exchange are so different the interfaces and protocols required to support them may differ. The interfaces and protocols used between the SA and the network, service or application are outside the scope of standardization related to UCI.

The PUA must maintain a current view on the communication possibilities across the range of networks, services and applications to which the user subscribes. Information describing this current status is maintained as part of the User Profile information in the PUA. Within the PUA there can be rules that look at the combined status information from across a range of services to which the UCI owner subscribes. The rules can build an integrated per-service view of the UCI owner (e.g. the combination of the PSTN and GSM Presence [9] and [10] Information can be used to build a view of the UCI owner's telephony status). These rules may also use various inference techniques to generate new information (e.g. information on whether the UCI owner is "using their computer at home" may be determined by examining any status information provided by the UCI owner's GSM service, to see if the owner is roaming, examining status information related to the PSTN subscriptions to see if the home PSTN telephone has recently been used and examining status information related to instant messaging subscriptions to see if the user is currently logged-in to their instant messaging application on their computer).

The table below shows some examples of how information gathered from services and other data sources (e.g. bank cash machines) could be used to build intelligent visions of the UCI owner's current communication environment.

Table 14: Examples of inferences from the application of information integration rules

	UK PSTN	GSM Mobile	Email	Bank	Inference
Case 1	On-hook - no recent activity	Terminal switched off	Last mail downloaded and read 1 hour ago	Withdrew cash in Munich 6 hours ago	Send all communications as email because telephony status is probably "unreachable"
Case 2	Off-hook 10 minutes ago	Terminal switched on and registered	Last mail downloaded and read 1 hour ago	No recent withdrawals	Try fixed line phone followed by mobile to minimize costs. Deliver email normally
Case 3	On-hook - no recent activity	On, roaming in France, recently used	No mail downloaded for 2 days	No information	Deliver email headers as well as voice calls to the mobile phone

12.3 PUA rules

The PUA contains a number of rules that are provided or chosen by the UCI owner. PUAs may provide UCI owners with applications that enable them to create PUA rules.

There are many possible formats for the rules and a similarly large range of potential mechanisms for processing them. In particular, the rules may be very complex or very simple and take into account a very narrow or a very wide range of possible factors in their execution. Typically, PUA rules will take into account such factors as the status of the UCI owner's services, the time of day and the identity of the person with whom the UCI owner is about to communicate.

It is perfectly possible to have PUAs interacting with other PUAs and SAs without putting any constraints on the content of the rules or on the methods by which they are processed. As such, the format of the rules and the mechanisms by which the rules are processed is not a matter for standardization and is thus outside the scope of the present document.

13 UCI Security Framework

Due to the universal nature of UCI, UCI systems will be operated not only with the current generation of communications technology but also with next generation networks (NGN) and legacy communication technology. Thus, when the security aspects of UCI systems were considered, all possible cases were considered. For example, Next Generation Networks (NGN) differ from current and previous generations of communications technology by breaking the relationship of the service with the access network. However when viewed as a security issue the NGNs exhibit new problems, primarily due to this separation.

In this clause, a UCI security framework will be established by using the following process:

1) Define security objectives for UCI systems.

2) Define a model for UCI security analysis.

3) Analyse threats to UCI systems and assess associated risks.

4) Define UCI security requirements.

5) Define UCI system security features and conduct a final risk assessment.

6) Give some suggestions on security mechanisms relevant to UCI systems.

13.1 Security Objectives Definition

In order to consider the security problems of UCI, it is important to understand what security is. One person's secure network is not the same as another's. In recognising this, some of the basic objectives to be met are outlined below. These objectives need to be tailored in every system and for every role. UCI complicates this somewhat by using a single user identifier for every role and across all systems.

13.1.1 General security objectives

In general, security objectives can be gathered into 5 main categories:

- Confidentiality
  - The avoidance of the disclosure of information without the permission of its owner.
- Integrity
  - The property that data has not been altered or destroyed in an unauthorized manner.
- Accountability
  - The principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation.
- Availability
  - The property of being accessible and usable upon demand by an authorized entity.
- Non-repudiation
  - A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

Therefore, threat analysis, risk assessment and the proposed countermeasures of any technology or service will be based on these objectives. However, some specific objectives specified in clauses 13.1.2, 13.1.3 and 13.1.4 may also be considered.

13.1.2 Users' objectives

The objectives of users are not uniform. An enterprise does not always require the same as a private person. The following list gives examples of possible objectives, which may have implications on security:

- availability and correct functionality of service subscription (including reachability, availability and correct functionality);
- correct and verifiable billing;
- data integrity;
- data confidentiality/privacy;
- capability to use a service anonymously;
- location confidentiality.

NOTE: This last objective may be relaxed to enable the provision of some location dependent services (subject to the user's agreement.

13.1.3 Service and network providers' objectives

The following list gives examples of objectives that may have implications on security:

- availability and correct functionality of network procedures;
- availability and correct functionality of service, network and element management;
- correct and verifiable billing and accounting, above all no possibility of fraud;
- non-repudiation for all network procedures and for all management activities;
- preservation of reputation (above all preservation of users' and investors' trust).

13.1.4 Manufacturers' objectives

The following list gives examples of objectives that may have implications on security:

- fulfilling market objectives;
- preservation of reputation.

13.1.5 UCI system security objectives

Based on the preceding discussion, in this clause the UCI system security objectives are listed in table 15.

Table 15: UCI System Security Objectives

General Security Objectives	UCI System Security Objectives
Confidentiality	**O1.** Confidentiality of the authentication information associated to a UCI **O2.** Confidentiality of the user presence information and location information **O3.** Confidentiality of user's profile
Integrity	**O4.** Integrity of user communication data is not compromised due to the introduction of UCI **O5.** Integrity of user profile **O6.** Integrity of billing data is not compromised due to the introduction of UCI
Accountability	**O7.** Accountability is not compromised due to the introduction of UCI
Availability	**O8.** Availability of PUA **O9.** Availability of SA
Non-repudiation	**O10.** Non-repudiation is not compromised due to the introduction of UCI

13.2 A Model for UCI Security Analysis

After reviewing the UCI system from the security perspective, a model for UCI security analysis is proposed as shown in figure 9.

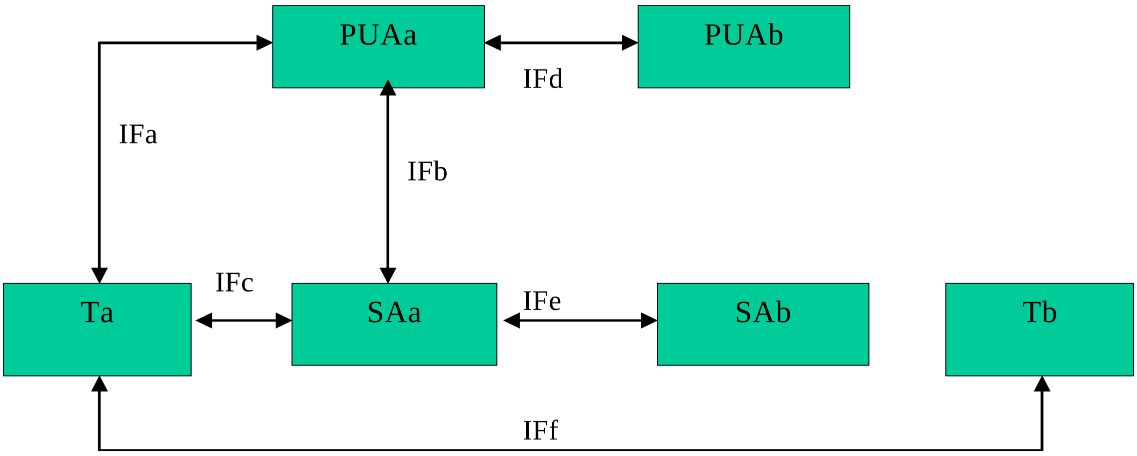


Figure 9: A model for UCI security analysis

This model defines assets to be protected in UCI systems, which include communication subjects, information flows, and functions and services. Detailed description of this model is given in clauses 13.2.1 through 13.2.4.

13.2.1 Communication subjects

There are three types of communication objects in this model:

- User terminal denoted as T.
- Personal user agent denoted as PUA.
- Service agent denoted as SA.

Ta, PUAa, and SAa are used to denote a user terminal and its associate PUA and SA. In this model, it is not necessary to distinguish an originating user from a target user. Ta can be an originator's terminal or a target user's terminal.

Tb, PUAb, and SAb are used to denote another user terminal, another PUA, and another SA respectively.

13.2.2 Information flow paths

There are six identifiable information flow paths:

- IFa: Bidirectional information flow path between a T and its PUA.
- IFb: Bidirectional information flow path between a PUA and an SA.
- IFc: Bidirectional information flow path between a T and its associated SA.
- IFd: Bidirectional information flow path between a PUA and another PUA.
- IFe: Bidirectional information flow path between an SA and another SA.
- IFf: Bidirectional information flow path between a T and another T.

13.2.3 Functions and services

The principal UCI functions and services for which security facilities may have to be provided are:

- PUA-PUA communication.
- PUA-SA communication.
- Discovery services.
- Presence/Availability services.
- Location-based services.
- Terminal registration and authentication.
- Communication set-up.
- User profile management.

13.2.4 Boundaries

For UCI security analysis purposes, the vertical boundary is set at the UCI function and service level. Network supporting functions at the lower layers are out of scope.

The horizontal boundary is the same as the core UCI system. For communication subjects, user terminals (Ta and Tb), PUAs and SAs are within the boundary. For information flows IFa, IFb, IFc, IFd and IFe are within the boundary. However, IFf is out of the boundary, since it represents the user communication data, which are supported by the communication services and networks, not by UCI functions and services.

13.3 Forms of Attack

In these clauses, general forms of attack relevant to UCI systems are presented.

13.3.1 Eavesdropping

Eavesdropping is a threat against confidentiality and is performed by intercepting the physical (or logical) link between the sender and the receiver. The decision to intercept a line will essentially depend on whether the information to be obtained will be worth the technical (financial) expenditure and the risk of being detected. The answer to this question is largely determined by the attacker's means and interests.

In most cases, eavesdropping is used to obtain data (e.g. such as user identification and authentication data) to be able to perform more serious threats at another point in time.

13.3.2 Masquerade

A perpetrator can use masquerading to feign a false identity. For instance, the perpetrator will obtain a false identity by spying out the user ID and password, by manipulating the originator field of a message, by manipulating the I/O address within the network, or simply by using another person's telephone or computer.

UCI is particularly susceptible in this area as it uses a single identity for all communication, and this identity is public.

A user who has been deceived as regards the identity of his communication partner can easily be persuaded to disclose sensitive information. Many email viruses work on this principle to propagate by using a forged identity and accessing a local address book to send attacks to known contacts.

A perpetrator can also use masquerading to try to tap an existing connection without having to authenticate himself, as this step has already been taken by the original participants in the communication (see also Eavesdropping in clause 13.3.1).

13.3.3 Replay

A message, or part of a message, is repeated to produce unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).

13.3.4 Modification of information

In this case, data is corrupted or rendered useless through deliberate manipulation. The consequences of this are the rejection of authorized accesses to network resources.

Attackers may be interested in modifying either the information required during the registration or the call set up phase. Reasons for this might be to use a service for which the attacked user has to pay.

Generally modification of information may be a starting point for denial of service or masquerade and fraud attacks.

13.3.5 Unauthorized access

Access to network entities must be restricted and conformant to the security policy in place. If attackers get unauthorized access to any of the network entities this could generally lead to various other attacks like denial of service, eavesdropping or masquerade. Likewise it is possible that unauthorized access is also a consequence of the other threats mentioned above.

13.3.6 Stalking

Stalking is using information to infer the whereabouts of a principal especially for malicious or illegal purposes. If the PUA and SA contain location data (particularly if bindings vary with location) this is a real threat.

13.3.7 Denial of service attacks

Denial of Service attacks (DoS), in particular Distributed Denial of Service (DDoS) attacks, strike at the physical networks used to host UCI services (PUAs and SAs) with the goal of consuming all of the target's network capacity and other resources including processes, CPU time, disk space, i-nodes, ports and directories.

DoS attacks will be aimed at preventing UCI users from using services or accessing devices that are normally available to them.

13.4 Threats to UCI System

Based on the general forms of attack, threats to UCI system are specified in table 16.

Table 16: Threats to UCI System

Threat Categories	Threat to UCI System	Rank of Threat
Eavesdropping	**T1.** Eavesdropping of IFa	Critical
	T2. Eavesdropping of IFb	Major
	T3. Eavesdropping of IFc	Critical
	T4. Eavesdropping of IFd	Critical
	T5. Eavesdropping of IFe	Major
Masquerade	**T6.** Masquerade of a user	Critical
	T7. Masquerade of a PUA	Minor
	T8. Masquerade of an SA	Minor
Replay	**T9.** Replay of IFa	Critical
	T10. Replay of IFb	Minor
	T11. Replay of IFc	Critical
	T12. Replay of IFd	Minor
	T13. Replay of IFe	Minor
Modification of information	**T14.** Modification of IFa	Major
	T15. Modification of IFb	Minor
	T16. Modification of IFc	Minor
	T17. Modification of IFd	Major
	T18. Modification of IFe	Minor
Unauthorized access	**T19.** Unauthorized access to user profile	Critical
Stalking	**T20.** Stalking	Critical
Denial of service	**T21.** Denial of PUA service	Critical
	T22. Denial of SA service	Major

In table 16, rank of each threat is assigned through risk assessment as detailed in annex E.

13.5 UCI System Security Requirements

From the results of risk assessment, the following security requirements can be specified.

R1. Information flow IFa should be protected from eavesdropping, replay, and modification.

R2. Information flow IFb should be protected from eavesdropping.

R3. Information flow IFc should be protected from eavesdropping, and replay.

R4. Information flow IFd should be protected from eavesdropping, and modification.

R5. Information flow IFe should be protected from eavesdropping.

R6. User's identity should be protected from masquerade.

R7. User profile should be protected from unauthorized access.

R8. Users should be protected from stalking.

R9. PUA should be protected from denial of service attack.

R10. SA should be protected from denial of service attack.

13.6 Countermeasures

Countermeasures have to be taken to contain the risk to an acceptable level. Most of these are simple in themselves.

13.6.1 Identification and authentication

In order to gain access to UCI services users will need to register an identity (private identity) and this identity shall be authenticated using methods based on secret key. Such methods are considered strong but do not authenticate a human user directly but only the device being used to gain service, however it may be possible to combine user input with a secret key method to more completely authenticate the user.

The authentication mechanism in UCI shall be mutual, i.e. user to PUA, PUA to user, and use as a time variant parameter a random number within a (mutual) challenge-response protocol.

Post authentication the private identity may be replaced with a temporary identity in like manner to the TMSI/IMSI relationship in GSM networks.

The identification and authentication methods described above will not be applicable to all instances where UCIs are used. Where users have to manually register their identity with their PUA (e.g. when wishing to communicate from a visited fixed line telephone) different methods for securely registering and de-registering will be required. Further studies will identify robust procedures for such registration/de-registration.

13.6.2 Encryption

Encryption in UCI can be used for the transfer of data between service elements to maintain confidentiality. The service elements at each end of the path shall generate the key used for encryption from the foregoing authentication exchange and an agreed method of getting time variance.

13.6.3 Cryptographic integrity

A cryptographic integrity mechanism can be used to protect information content from being modified in an unauthorized manner.

13.6.4 Protection from denial of service attacks

It is not possible to guarantee protection from DoS attack but UCI and the framework for communication that it uses can mandate some variants of the following basic protections:

- Filtering at network ingress (IETF RFC 2267 [3]);
- Filtering at network egress;
- Disabling of directed broadcast (IETF RFC 2644 [11]);
- Media Anti-spamming method for RTP channels.

13.6.5 Intrusion detection systems

Intrusion detection systems help an organization by:

- determining that it is (potentially) under attack;
- identifying the nature of the attack;
- suggesting responses to the attack or responding automatically to the attack (the automated response can be tailored by the organization);
- collecting evidence of the attack;

- providing some data on the identity of the attacker (although the attacker may have taken measures to make himself anonymous or may have a stolen identity).

13.6.6 Location specific service binding

If a user is mobile he has to modify his UCI to service bindings (in order to bind his UCI to the service and thus to the network availability of the service at his current location). These bindings have to be revoked on each new binding. Safe revocation has to be ensured.

Timed authorization tickets for each binding may present a solution to this problem.

13.7 UCI System Security Features

The following security features are necessary to protect UCI system from all critical and major threats and reduce the risk to the acceptable level.

F1. Apply strong authentication for a user terminal to access its PUA and SA.

F2. Use time variant parameters for authentication.

F3. Encryption of information flows between a T and its PUA.

F4. Encryption of information flows between a PUA and an SA.

F5. Encryption of information flows between a T and its associated SA.

F6. Encryption of information flows between a PUA and another PUA.

F7. Encryption of information flows between an SA and another SA.

F8. Cryptographic integrity checking mechanism for information flows across relationship IFa.

F9. Cryptographic integrity checking mechanism for information flows across relationship IFd.

F10. Protection of PUA from denial of service attacks.

F11. Protection of SA from denial of service attacks.

F12. Intrusion detection system for PUA provider

F13. Safe revocation of location specific service binding

13.8 Threats after application of countermeasures

Table 17 shows how, after application of properly designed security features (see clause 13.7) the rank of the threats shown in table 16 change significantly.

Table 17: Threats to UCI System after application of UCI system security features

Threat Categories	Threat to UCI System	Rank of Threat
Eavesdropping	**T1.** Eavesdropping of IFa	Minor
	T2. Eavesdropping of IFb	Minor
	T3. Eavesdropping of IFc	Minor
	T4. Eavesdropping of IFd	Minor
	T5. Eavesdropping of IFe	Minor
Masquerade	**T6.** Masquerade of a user	Minor
	T7. Masquerade of a PUA	Minor
	T8. Masquerade of an SA	Minor
Replay	**T9.** Replay of IFa	Minor
	T10. Replay of IFb	Minor
	T11. Replay of IFc	Minor
	T12. Replay of IFd	Minor
	T13. Replay of IFe	Minor
Modification of information	**T14.** Modification of IFa	Minor
	T15. Modification of IFb	Minor
	T16. Modification of IFc	Minor
	T17. Modification of IFd	Minor
	T18. Modification of IFe	Minor
Unauthorized access	**T19.** Unauthorized access to user profile	Minor
Stalking	**T20.** Stalking	Minor
Denial of service	**T21.** Denial of PUA service	Minor
	T22. Denial of SA service	Major

Table 17 shows that the security features proposed in clause 13.7 are effective to reduce the risk to an acceptable level. This means the resulting UCI system addresses those risks and may be considered resistant to attack in those areas.

13.9 Security Mechanisms

Annex D contains a description of 3 types of security mechanism that may be relevant to UCI-based systems:

- Public, Private and Secret keys;
- Internet Key Exchange (IKE) [4];
- Digital signature.

14 Administrative issues

Not all of the issues in the delivery of an effective UCI system relate to the technical design of the system. There are a number of administrative issues that need to be solved to enable a UCI system to function. Such issues include:

- the authorities and the processes involved in the creation and allocation of UCIs;
- the authorities and the processes involved in the authentication of UCIs, PUAs, SAs, etc.;
- the agreements that will be needed between the various authorities responsible for the elements of the UCI system (to assure such things as the privacy of user information).

There are many parallels between the issues that are of importance in the administration of an ENUM system (see annex F) and the administration of UCI. For this reason, the work in SPAN11 on "ENUM administration in Europe" is being closely followed and contributed to by STF180.

As the SPAN11activity has wide participation from ENUM service providers, telecommunications service providers and European national regulators, it is likely that the model being formulated can command wide support within Europe. International support for this model is also likely as the ETSI work is based upon similar work being undertaken within the USA. For this reason, the SPAN11 administrative model should act as a very solid basis from which to consider the development of a UCI model.

15 Key standards activities

Annex C shows that a number of standards bodies are working in areas closely aligned with many of the key UCI Technical Requirements. The most significant standards activities that relate closely to UCI are:

Table 18: Key standards activities

Standards Bodies	Activities of relevance of UCI
TIPHON	Overall architecture, registration processes, security issues, naming and addressing.
ETSI SPAN11, ITU-T SG2	Naming, numbering, addressing, routing, telecommunications supplementary services, ENUM administration.
IETF ENUM	ENUM's role in resolving an E.164 telephone number into another identifier (that can be used for routing) makes this topic of high importance in relation to resolving the numeric element of a UCI into a routing address to the PUA.
IETF IMPP, 3GPP Presence, PAM Forum	The need for the SA to know about the status of the user and the user's services makes this group of standards particularly relevant.
SPAN 14 (SPAR), 3GPP OSA, PARLAY and JAIN™	As these activities relate to the ability of a 3rd party (in the case of UCI a PUA) to control a network or service (in the case of UCI a SA) this activity is of critical relevance to the operation of UCI.
ETSI TC HF	The ability of users to communicate and to manage their communications with the maximum ease of use is of critical importance to the success of UCI. Many of the activities in the work of TC HF (including its specific work on UCI being done in STF200) is of vital importance to the success of UCI.
FIPA	FIPA define how intelligent agents can intercommunicate and negotiate a mutually acceptable outcome. This is precisely the activity that negotiating PUAs will need to do.
ITU-T SG13	As ITU-TSG13 cover standardization activity for future communications systems, they cover many of the topics that systems communicating with UCI need to address.

Throughout the development of the UCI, the standards activities of the above bodies have been examined carefully and active participation in many of these activities has taken place.

Annex A (informative): UCI Scenarios

A.1 Introduction

The following scenarios illustrate the way that key user requirements are satisfied by using the UCI. The scenarios:

- illustrate the potential usage of UCls in a number of easy-to-follow descriptions of everyday communications related tasks;
- provide a number of test-cases against which the emerging architecture described in the present document can be evaluated.

The scenarios are presented in a multi-column layout in such a way that it is possible to identify the UCI-related activity that leads to key behaviour described in the text of the scenario. Although closely aligned with the main description of UCI in this present document, the flows shown are for illustrative purposes only.

All the scenarios illustrate the core UCI behaviour described in clause 6. Additional capabilities beyond this core capability (e.g. conference bridges and text messaging based email notification services) are shown in the scenarios in order to illustrate the potential power of UCI when used at the heart of a richer communications environment.

A.2 Mobile Worker Scenario

A.2.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- how information on the current state of the UCI owners communications services is used by the PUA to choose the appropriate communication service and terminal for the incoming communication it is trying to negotiate (Step 1);
- the way in which the basic UCI communication process is adapted for email in a way that avoids large-scale adaptation of current email delivery mechanisms (e.g. mail servers and the SMTP protocol) (Step 2);
- the way in which the PUA is able to route communications to services that lie outside the scope of UCI, as defined by the present document, in order to have an email translated into a fax and then subsequently delivered (Step 3).

A.2.2 Scenario description

Two fundamental user requirements of communications are that network boundaries should be invisible to users and that user interfaces should be unified. This scenario illustrates in a simple example how such attributes, delivered by a UCI based communication architecture, enhance the efficiency of a mobile worker.

In this scenario, the character Francois spends half his time in the office and half on the road visiting clients. He has a work mobile phone and at the office he has a fixed phone line and a networked PC.

Table A.1: Mobile Worker Scenario

Scenario Description	Technical Notes
STEP 1 An incoming call from a customer Mr. Dubois is routed to his fixed line telephone. The customer wants some advice and is asked to email this particular query as it involves detailed numeric data.	PUA knows he is probably at his desk because he is logged on at his PC. This information may be provided by a Presence Service.
STEP 2 Francois logs off and goes off in his car to visit other customers. Mr. Dubois sends the email. This is automatically formatted as an SMS message and sent to Francois's mobile phone. The message requests that any response is in the form of a fax.	The PUA knows that Francois is not logged on and is therefore likely to be out of the office. It initiates a service which formats the email as SMS messages and sends these.
STEP 3 A little later Francois, sitting in his car, has produced a response to Mr. Dubois's query. He uses the communication history function to select "Mr Dubois" and then constructs a text reply. When the send instruction is selected, the display offers the option of sending as SMS (default), email or fax. Francois sends the reply as fax, as requested by his customer.	The range of options offered (SMS, email or fax) will be determined by the services that Francois is entitled to use from the SA to which he is attached. The chosen service will be communicated to the terminating PUA in the communication request message.

A.2.3 Discussion

A.2.3.1 Step 1 - Incoming call whilst Francois is in the office

Francois is in his office using his computer. An incoming call from Mr. Dubois, a customer, is routed to his fixed line telephone. The customer wants some advice and is asked to email this particular query as it involves detailed numeric data.

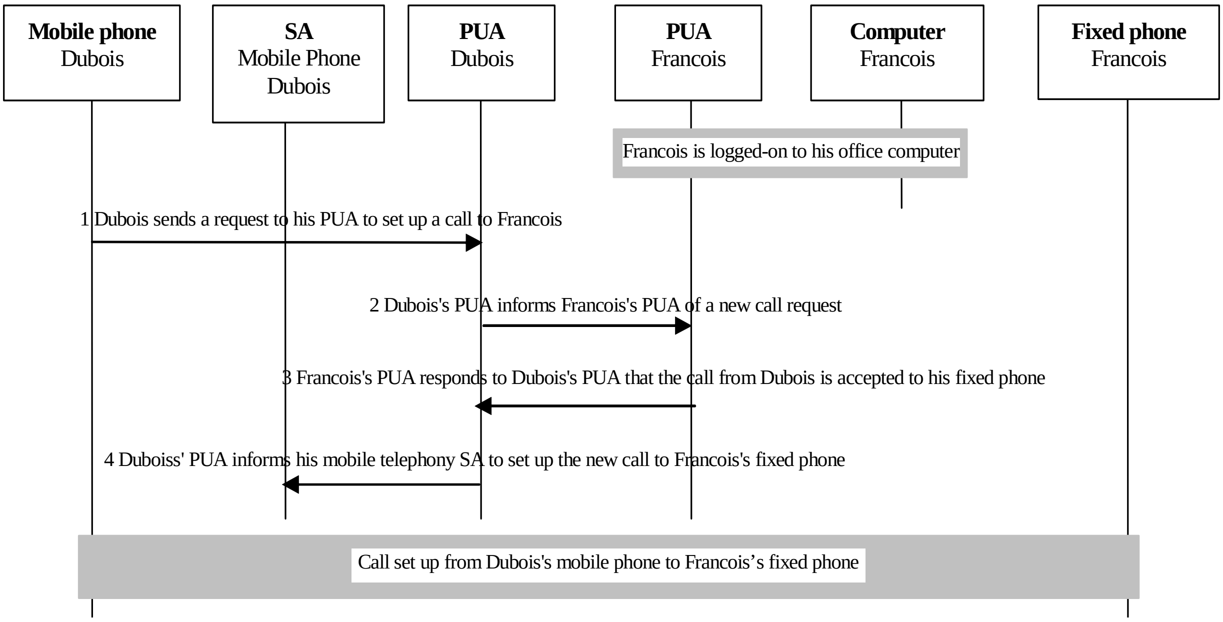

Mobile phone Dubois
SA Mobile Phone Dubois
PUA Dubois
PUA Francois
Computer Francois
Fixed phone Francois
Francois is logged-on to his office computer
1 Dubois sends a request to his PUA to set up a call to Francois
2 Dubois's PUA informs Francois's PUA of a new call request
3 Francois's PUA responds to Dubois's PUA that the call from Dubois is accepted to his fixed phone
4 Duboiss' PUA informs his mobile telephony SA to set up the new call to Francois's fixed phone
Call set up from Dubois's mobile phone to Francois’s fixed phone

Figure A.1: Mobile Worker Scenario - Step 1 - Incoming call while Francois is in the office

Flow	Parameters	Action
As Francois is logged-in to his computer and as he is actively using it. From this his PUA knows that he is in the office.		
1 Dubois sends a request from his mobile phone to his PUA to set-up a call to Francois	Called Party Identity = Francois UCI <numeric> Service Type = P-P real-time voice QoS = GSM Voice	Dubois makes a call request to Francois's UCI.
2 Dubois's PUA informs Francois's PUA of a new call request	Called Party Identity = Francois UCI <numeric> Calling Party Identity = Dubois UCI <label; numeric> Command = Call request Service Type = P-P real-time voice QoS = GSM Voice	Dubois PUA negotiates with Francois's PUA for the call.

3 Francois's PUA responds to Dubois's PUA that the call from Dubois is accepted	Called Party Identity = Francois UCI <label, numeric>
	Called Party Identity = Dubois UCI <label, numeric>
	Command = Accept call
	Service Type = P-P stored voice
	QoS = GSM/PSTN Voice
	Data = Routing information for Francois's fixed (office) telephone
		Francois PUA knows he is in the office and offers to accept the call on his fixed office phone.

4 Dubois' PUA informs Dubois's mobile telephony SA to set up the new call request	Calling Party Identity = Dubois UCI <label, numeric>
	Called Party Identity = Francois UCI <label, numeric>
	Command = Establish call
	Service Type = P-P stored voice
	QoS = GSM/PSTN Voice
	Data = Routing information for Francois's fixed (office) telephone
		The network is supplied sufficient information to set up the call between Dubois's mobile phone and Francois's fixed office telephone.

A Call is set up from Dubois' mobile phone to Francois' fixed office phone. During the conversation a decision is made that Dubois needs to send a detailed advice query as an email.		

Step 1 - Issues

- Francois has agreed that his own PUA (only) can be informed that he is actively using his PC. His PUA can use this information to make more appropriate decisions when delivering communications to him.

- Francois's PUA must have the rule to use the fixed phone for incoming calls when Francois is logged onto and using the office computer.

A.2.3.2 Step 2 - Incoming email whilst Francois is out of the office

Francois logs off and goes off in his car to visit other customers. Mr. Dubois sends the email.

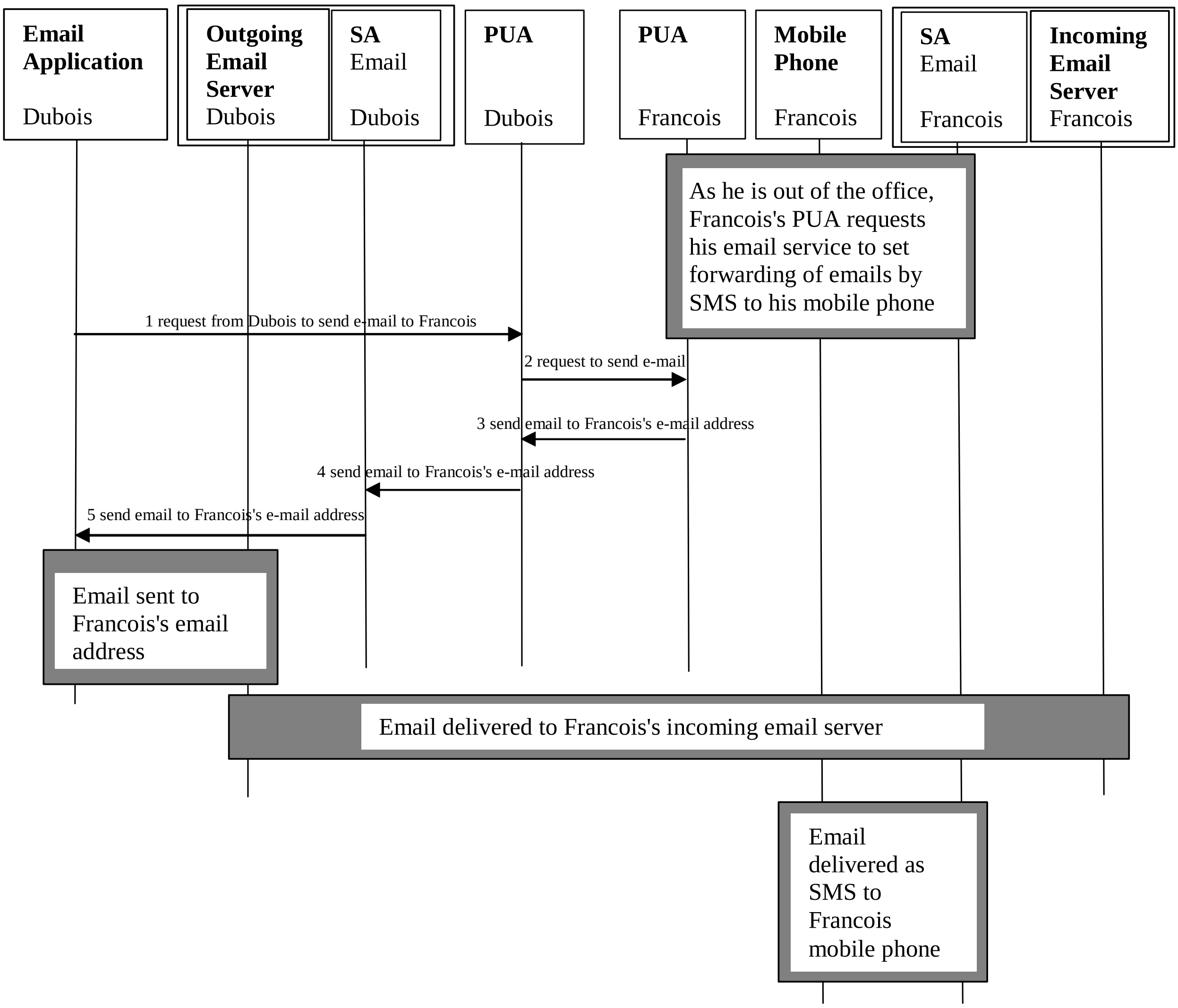

Email Application Dubois
Outgoing Email Server Dubois
SA Email Dubois
PUA Dubois
PUA Francois
Mobile Phone Francois
SA Email Francois
Incoming Email Server Francois
As he is out of the office, Francois's PUA requests his email service to set forwarding of emails by SMS to his mobile phone
1 request from Dubois to send e-mail to Francois
2 request to send e-mail
3 send email to Francois's e-mail address
4 send email to Francois's e-mail address
5 send email to Francois's e-mail address
Email sent to Francois's email address
Email delivered to Francois's incoming email server
Email delivered as SMS to Francois mobile phone

Figure A.2: Mobile Worker Scenario - Step 2 - Incoming email whilst Francois is out of the office

Flow	Parameters	Action
When Francois leaves the office he logs out of his computer. His PUA interprets this as him being out of the office and sends a request to his email service to forward all emails to his mobile phone.		
1 Dubois sends a request to his PUA to send an email to Francois	Called Party Identity = Francois UCI <numeric> Service Type = Email	Dubois sends an email to Francois's UCI.
2 Dubois's PUA informs Francois's PUA of an email request	Called Party Identity = Francois UCI <numeric> Calling Party Identity = Dubois' UCI <label; numeric> Command = Email request Service Type = Email	Dubois' PUA negotiates with Francois's PUA to obtain an email acceptance.
3 Francois's PUA responds to Dubois' PUA that the email should be sent to Francois's email address	Called Party Identity = Francois UCI <label, numeric> Calling Party Identity = Dubois UCI <label; numeric> Command = Accept email Service Type = Email Data = Routing information for Francois's email account	Francois's PUA knows which email accounts he is likely to be reading and sends details of one of them in return.
4 Dubois's PUA requests his email service to send an email to Francois's email account	Calling Party Identity = Dubois UCI <label; numeric> Called Party Identity = Francois UCI <label, numeric> Command = Send email Service Type = Email Data = Routing information for Francois's email account	The email service is supplied sufficient information to direct the email to Francois's chosen account.

5 Dubois's email service provides the destination information and initiates the send action	Called Party Identity = Francois's email account
	Command = Send
	Message = Message Dubois entered
	Attachment = Dubois's UCI
		Dubois's email service supplies the information to populate the "To" field of the email and also Dubois's UCI as an email attachment.

NOTE 1: An email is sent from Dubois's Email application to his Outgoing Email Server. NOTE 2: Dubois' outgoing email server delivers the email to Francois's incoming email server. NOTE 3: Francois's email service formats the incoming email from Dubois as an SMS message and sends it to Francois's mobile phone (as earlier instructed by Francois's PUA).		

Step 2 - Issues

- Francois's PUA has a rule that interprets logging out of his PC as an indication that Francois is out of the office and will be receiving all communications on his mobile phone.

- Francois's email service must have the facility to format email messages as SMS messages and send them to Francois's mobile phone.

- The approach in this scenario where the email service has an inbuilt email to SMS feature contrasts with that in clause A.4.2.6 where the PUA of the recipient is invoked to deliver an incoming email as a fax by invoking an email to fax conversion service.

A.2.3.3 Step 3 - Responding to Dubois's original email

A little later Francois, sitting in his car, has produced a response to Mr. Dubois's query. He uses the communication history function to find the last communication from "Mr Dubois" and then constructs a reply in SMS format. When the send instruction is selected, the display offers the option of sending as SMS (default), email or fax. Francois selects the "reply as fax" option, as requested by his customer.

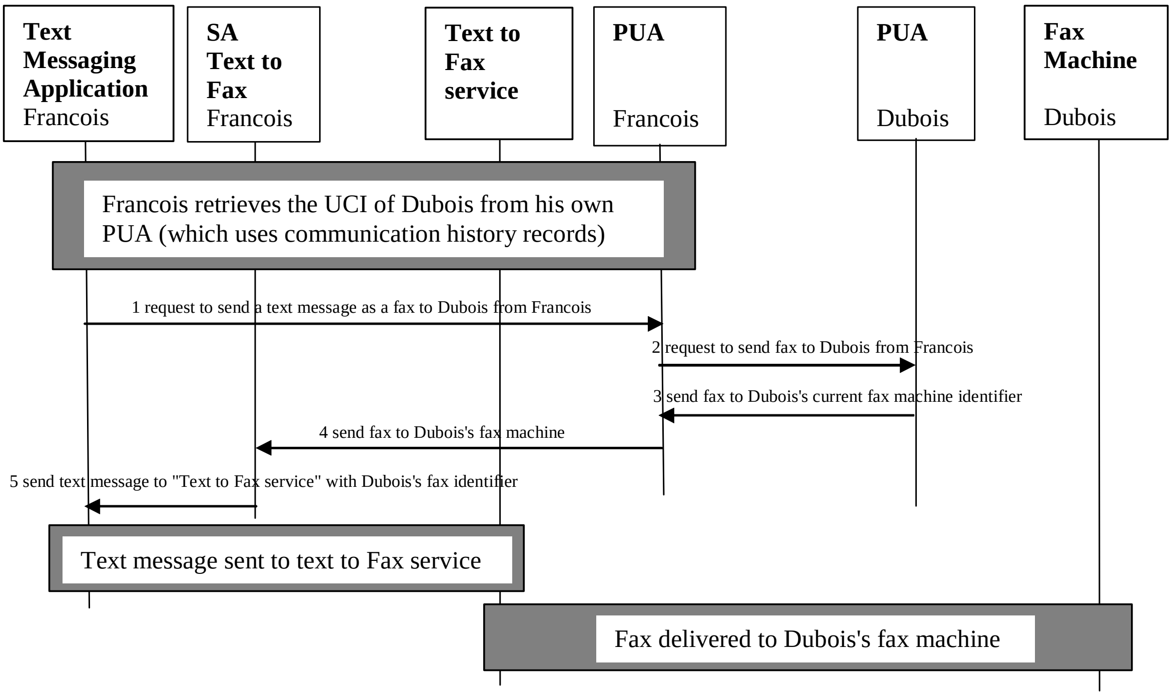

Text Messaging Application Francois
SA Text to Fax Francois
Text to Fax service
PUA Francois
PUA Dubois
Fax Machine Dubois
Francois retrieves the UCI of Dubois from his own PUA (which uses communication history records)
1 request to send a text message as a fax to Dubois from Francois
2 request to send fax to Dubois from Francois
3 send fax to Dubois's current fax machine identifier
4 send fax to Dubois's fax machine
5 send text message to "Text to Fax service" with Dubois's fax identifier
Text message sent to text to Fax service
Fax delivered to Dubois's fax machine

Figure A.3: Mobile Worker Scenario - Step 3 - Responding to Dubois's original email

Flow	Parameter	Action
Francois accesses the communication log records to locate the last communication form Dubois. This provides Dubois UCI to be used in the communication described here.		
1 Francois sends a request to his PUA to send his text message as a fax Dubois	Called Party Identity = Dubois UCI <numeric> Service Type = Fax QoS =	Dubois requests that a fax be sent to Dubois using the context of the text in Francois's text messaging application.
2 Dubois' PUA informs Francois' PUA of an email request	Called Party Identity = Dubois UCI <numeric> Calling Party Identity = Francois' UCI <label; numeric> Command = Fax Service Type = Fax QoS =	Francois's PUA negotiates with Dubois' PUA to obtain a fax number for Dubois.
3 Dubois's PUA responds to Francois's PUA that the fax should be sent to Dubois's fax number	Called Party Identity = Dubois UCI <label, numeric> Calling Party Identity = Christine UCI <label; numeric> Command = Accept email Service Type = Fax QoS = Data = Routing information for Dubois's fax machine	Dubois PUA sends details of the number of his fax machine
4 Francois's PUA requests the text to fax service to send the fax to Dubois's fax machine	Calling Party Identity = Francois UCI <label; numeric> Called Party Identity = Dubois' UCI <label, numeric> Command = Send email via text to fax service Service Type = Fax QoS = Data = Routing information to the fax service and for Dubois's fax machine	The details of Dubois fax machine are forwarded to the text to fax service.

5 The text to fax service provides its own and Dubois destination information and initiates the send action	Called Party Identity = Francois's email account
	Command = Send
	Message = Message Francois entered + Francois's UCI
		The text to fax service supplies its own identity to the text messaging application. It also supplies Francois's UCI information for forwarding to the Dubois's fax.

NOTE 1: A text message together with Francois's UCI is sent from Francois's text messaging application to the text to fax service. NOTE 2: The text message and UCI are sent to Dubois as a fax.		

A.3 Home Scenario

A.3.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- the PUA's ability to instruct an application to generate an SMS message to alert its user to an incoming email (Step 1);
- the management of aspects of a PUA profile by its UCI owner (Step 2);
- preservation of the privacy of UCI owners according to the criteria they set via their PUAs. In this example a technique called a Virtual Calling Card is used (Step 3);
- the PUA's ability to request distinctive user alerting dependant on the UCI identity of the recipient (Step 4);
- registration of a UCI owner at a terminal belonging to someone other than the UCI owner (Step 5).

A.3.2 Scenario description

This scenario illustrates a situation which will be commonplace in a residential environment where more than one person shares a terminal. People will be able to create a user profile which defines the appropriate level of privacy given their circumstances at any given time. Different people in the same dwelling could easily define different levels of privacy. Access to UCI directory listings will also be subject to access rules defined by the UCI owner.

Jenny and Mike Smith live in the same house and each have their own personal UCI/PUA. They have their own mobiles but share a fixed telephone, PC and fax machine.

Table A.2: Home Scenario

Scenario Description	Technical Notes
BACKGROUND	
Jenny and Mike Smith live in the same house and each have their own personal UCI/PUA. They have their own mobiles but share a fixed telephone, PC and fax machine.	Separate PUAs per person, separate SAs per service/network subscription. Registration needed to SAs and then PUAs. The fixed telephony SA needs to know about Mike's PUA and Jenny's PUA.
STEP 1 Jenny wants to make a telephone call to her friend Lucy. She presses her own dedicated special identification button on the telephone and then scrolls through her customized address book on the small display. She selects Lucy and presses a "dial" button. Lucy is not available at the moment but a network-based service offers to take a short voice message. Lucy gets an SMS telling her that she has a new voice message.	This requires a specialized phone. Implies that users may not opt to have PIN confirmation as an additional identification confirmation (see note). Cf security levels on Win95 vs WIN NT user accounts. Lucy's PUA is set to send her an SMS message when she gets new voicemail.
STEP 2 Mike is trying to work at home and is fed up with telephone sales calls interrupting him. He accesses his PUA profile management application via the Internet and sets his preferences to only accept calls during the afternoon coming from his work and urgent calls from family and friends. All other calls will be diverted to his voice messaging service for him to review later.	Mike uses his PC to access the user profile management application of his PUA and change some call screening options. The PUA recognizes the priority categories defined by such bodies as the ITU-T Recommendation E.106. The categories "work", "family" and "friends" have already been pre-defined. These categories will contain a list of UCIs and also telephone numbers, email addresses, etc.
STEP 3 In the evening Mike wants to get hold of an old school friend and uses his PC based UCI search tool. The directory search determines that his friend has set his UCI Privacy Protection so that an unknown person can leave a "virtual calling card" consisting only of the callers UCI and reason for communication. Mike selects "friend" and "call me back" categories from the available options.	The standard "virtual calling card" would automatically complete the UCI field and offer a set of pre-set categories for reason for communication (e.g. relative, friend, customer) and required action (e.g. "call me back" or "send me your UCI").
STEP 4 Eventually his old friend John Fields calls him back in the evening. Mike recognizes his personal ringing tone on an incoming call and sees the name "John Fields" clearly shown on the telephone display - so he takes the call.	This implies that a distinctive ringing supplementary service has been invoked (for Jenny and Mike's fixed telephony service) to associate different tones with calls to different UCIs. The name shown is the UCI label (which the PUA/network must be capable of delivering and the terminal must be capable of displaying). Provision for withholding or releasing the numeric (and other) elements of the UCI should be supported.
STEP 5 Next day John arrives at Mike and Jenny's and decides to stay overnight at short notice. He wants to call a few people to tell them what he's doing. John puts his Smart Card in the telephone's reader. His own address book is now available and he makes the required phone calls.	This ensures that calls are booked to John's account, that John's PUA knows the identification of the terminal, that he has access to his own personal address book and that his UCI is given out as the originator of his communications. The use of the Smart Card permits a short-term override of the PUA defaults to be made without the user needing to manually change PUA preference settings.
NOTE: The other party can request the caller to verify identification.	

A.3.3 Discussion

A.3.3.1 Step 1 - Jenny makes outgoing call

Jenny wants to make a telephone call to her friend Lucy. She presses her own dedicated special identification button on the telephone and then scrolls through her customized address book on the small display. She selects Lucy and presses a "dial" button. Lucy is not available at the moment but a network-based service offers to take a short voice message. Lucy gets an SMS telling her that she has a new voice message.

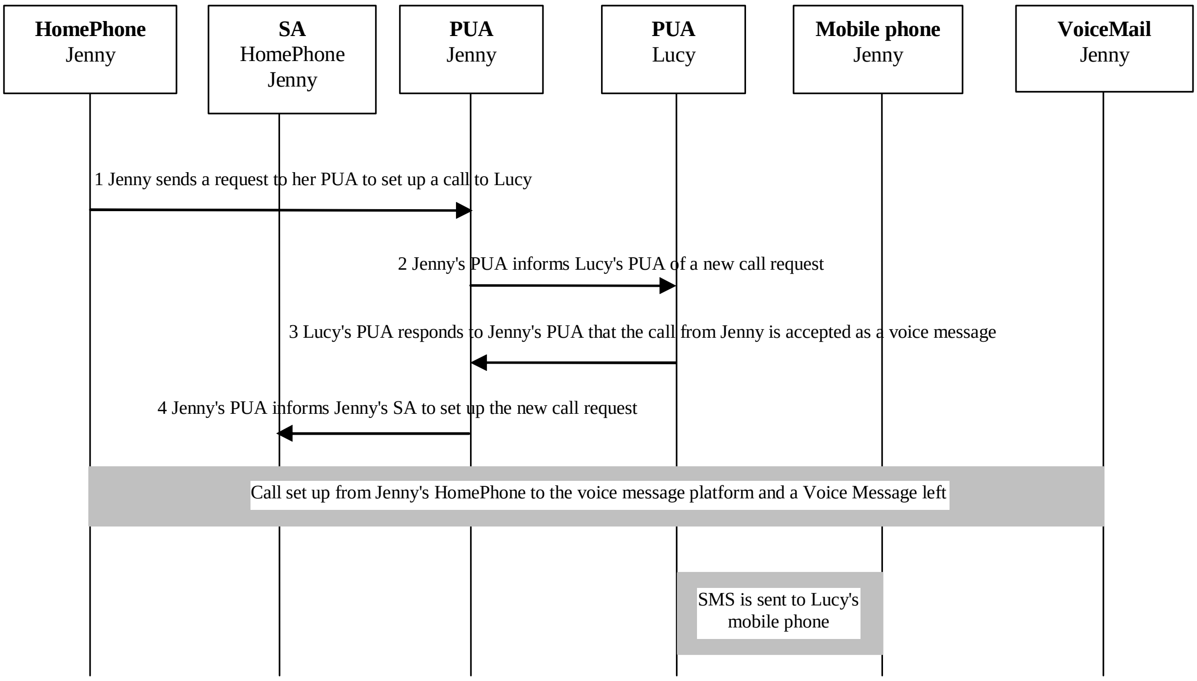

HomePhone Jenny
SA HomePhone Jenny
PUA Jenny
PUA Lucy
Mobile phone Jenny
VoiceMail Jenny
1 Jenny sends a request to her PUA to set up a call to Lucy
2 Jenny's PUA informs Lucy's PUA of a new call request
3 Lucy's PUA responds to Jenny's PUA that the call from Jenny is accepted as a voice message
4 Jenny's PUA informs Jenny's SA to set up the new call request
Call set up from Jenny's HomePhone to the voice message platform and a Voice Message left
SMS is sent to Lucy's mobile phone

Figure A.4: Home Scenario - Step 1 - Jenny makes outgoing call

Flow	Parameters	Action
1 Jenny sends a request to her PUA to set-up a call to Lucy	Called Party Identity = Lucy UCI <numeric> Service Type = P-P real-time voice QoS = PSTN Voice	Jenny makes a call to Lucy's UCI.
2 Jenny's PUA informs Lucy's PUA of a new call request	Called Party Identity = Lucy UCI <numeric> Calling Party Identity = Jenny UCI <label; numeric> Command = Call request Service Type = P-P real-time voice QoS = PSTN Voice	Jenny's PUA negotiates with Lucy's PUA for the call.
3 Lucy's PUA responds to Jenny's PUA that the call from Jenny is accepted as a voice message	Called Party Identity = Lucy UCI <label, numeric> Called Party Identity = Lucy UCI <label, numeric> Command = Accept call Service Type = P-P stored voice QoS = PSTN Voice Data = Routing information for Lucy's voice message server	Lucy's PUA knows she is not available but a network-based service is offered to take a short voice message.
4 Jenny's PUA informs Jenny's SA to set up the new call request	Calling Party Identity = Jenny UCI <label, numeric> Called Party Identity = Lucy UCI <label, numeric> Command = Establish call Service Type = P-P stored voice QoS = PSTN Voice Data = Routing information for Lucy's voice message server	The network is supplied sufficient information to set up the call between Jenny's terminal and Lucy's voice message server.
NOTE 1: A Call is set up from Jenny's Home Phone to the voice message platform. A voice message is left for Lucy. NOTE 2: Lucy's PUA ensures that an SMS telling her that she has a new voice message is sent. Parameters are supplied by the originating call or her PUA		

Step 1 - Issues

- Lucy's PUA must know she is unavailable to receive voice calls.
- Lucy's PUA must redirect call to her voice message service.
- A local or remote application will send the SMS under instruction from the PUA.
- Lucy's PUA must receive sufficient details about the voice message to ensure a satisfactory SMS is sent to Lucy's mobile phone.

A.3.3.2 Step 2 - Mike updates his profile

Mike is trying to work at home and is fed up with telephone sales calls interrupting him. He accesses his PUA profile management application via the Internet and sets his preferences to only accept calls during the afternoon coming from his work and urgent calls from family and friends. All other calls will be diverted to his voice messaging service for him to review later.

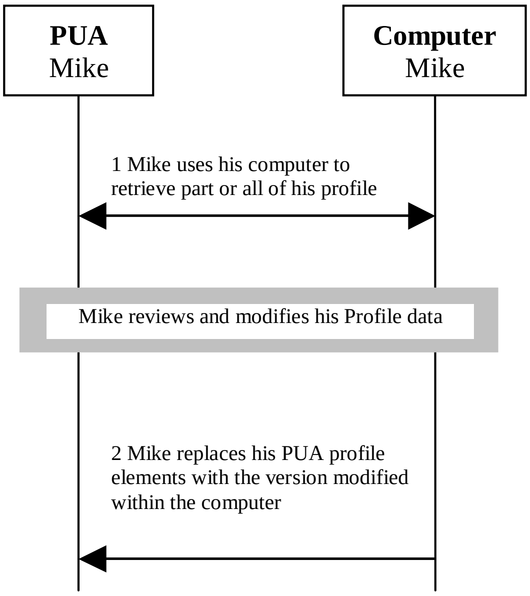

PUA
Mike
Computer
Mike
1 Mike uses his computer to retrieve part or all of his profile
Mike reviews and modifies his Profile data
2 Mike replaces his PUA profile elements with the version modified within the computer

Figure A.5: Home Scenario - Step 2 - Mike updates his profile

Flow	Parameters	Action

1 Mike uses his computer to retrieve part or all of his profile from his PUA	User identity = Mike UCI
	Command = Get
	Source = Mike's PUA Profile rules
	Item = Incoming call screening
	Authentication =
		Mike requests the Incoming call screening section of his personal profile from his PUA. He then reviews and amends in accordance with his personal preferences regarding incoming call screening. The PUA responds by returning the appropriate personal profile elements. He then reviews and amends in accordance with his personal preferences regarding incoming call screening.

Mike reviews and modifies his profile data		

2 Mike replaces his PUA profile elements with the modified version	User identity = Mike UCI
	Command = Replace
	Source = Mike's PUA Profile rules
	Item = Incoming call screening
	Authentication =
		The Incoming call screening elements of the PUA version of the personal profile is replaced by the amended local version stored on Mike's computer

Step 2 - Issues

- Mike's PUA must apply authentication/security procedures on the get profile request.
- Mike's PUA must apply authentication/security procedures on the replace profile request.

A.3.3.3 Step 3 - Mike searches for 'old school friend'

In the evening Mike wants to get hold of an old school friend and uses his PC based UCI search tool. The directory search determines that his friend has set his UCI Privacy Protection so that an unknown person can leave a "virtual calling card" consisting only of the caller's UCI and reason for communication. Mike selects "friend" and "call me back" categories from the available options.

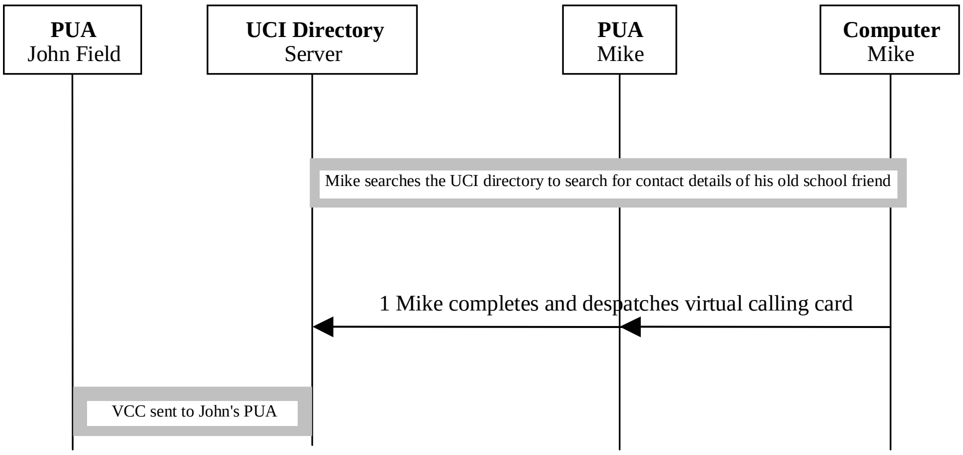

PUA
John Field
UCI Directory
Server
PUA
Mike
Computer
Mike
Mike searches the UCI directory to search for contact details of his old school friend
1 Mike completes and despatches virtual calling card
VCC sent to John's PUA

Figure A.6: Home Scenario - Step 3 - Mike searches for 'old school friend'

Flow	Parameters	Action
Mike requests contact details of his 'old school friend'. This could be a proprietary www-based application The search application returns via the PUA, the stored contact details on Mike's 'old school friend' who has set his UCI Privacy Protection so that an unknown person can leave a "virtual calling card" consisting only of the callers UCI and reason for communication.		
1 Mike completes and despatches virtual calling card	User identity = Mike UCI <label; number> Authentication =	Mike selects the options "friend" and "call me back" categories from the virtual calling card and his PUA automatically supplies his UCI name and identification credentials.
NOTE: The UCI directory server forwards the completed "virtual calling card" to John's PUA		

Step 3 - Issues

- The www-based database must contain fields for private communication (ex directory) whilst offering a virtual calling card return service.
- Such enhanced functionality is easier to provide when the search uses peer-to-peer searching between PUAs (or PUA Providers) than when the search is on a conventional database or directory system.
- Mike's PUA must apply authentication/security procedures for completing the virtual calling card.

A.3.3.4 Step 4 - 'Old school friend' returns call

Eventually his old friend John Fields calls him back in the evening. Mike recognizes his personal ringing tone on an incoming call and sees the name "John Fields" clearly shown on the telephone display - so he takes the call.

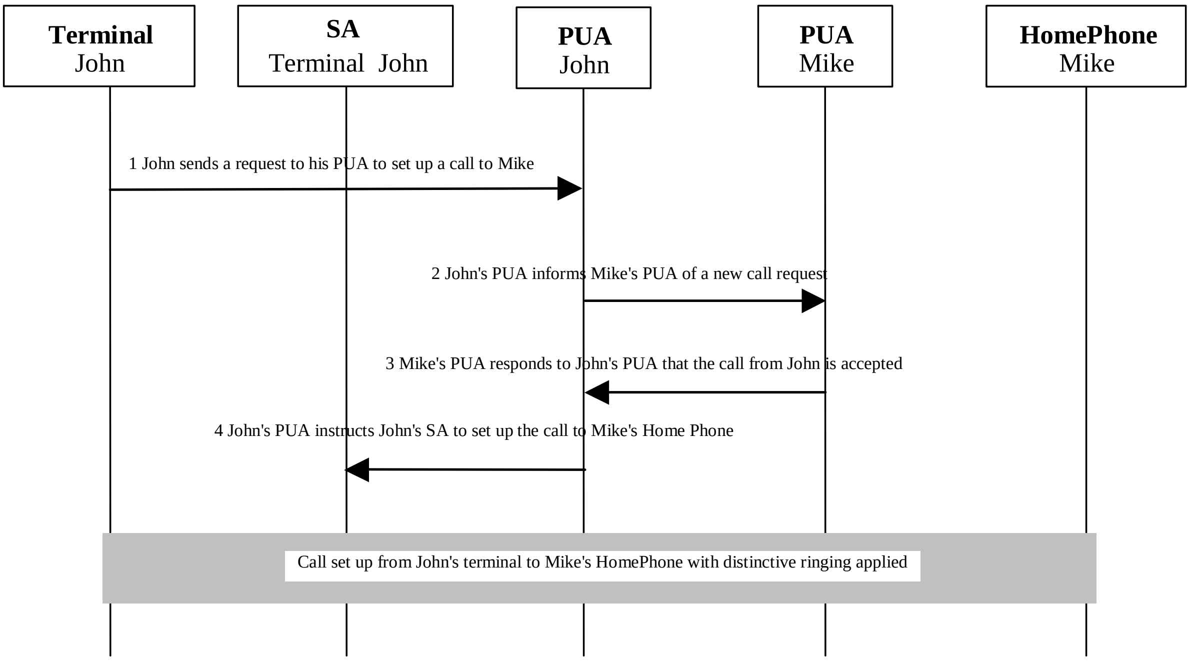

Terminal
John
SA
Terminal John
PUA
John
PUA
Mike
HomePhone
Mike
1 John sends a request to his PUA to set up a call to Mike
2 John's PUA informs Mike's PUA of a new call request
3 Mike's PUA responds to John's PUA that the call from John is accepted
4 John's PUA instructs John's SA to set up the call to Mike's Home Phone
Call set up from John's terminal to Mike's HomePhone with distinctive ringing applied

Figure A.7: Home Scenario - Step 4 - 'Old school friend' returns call

Flow	Parameters	Action
1 John sends a request to his PUA to set up a call to Mike	Called Party Identity = Mike UCI <number> Calling Party Identity = John Fields UCI <label; number =withheld> Service Type = P-P real-time voice QoS = PSTN voice	John Fields initiates a call to Mike.
2 John's PUA informs Mike's PUA of a new call request	Called Party Identity = Mike UCI <number> Calling Party Identity = John Fields UCI <label; number =withheld> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	John Field's PUA offers a call to Mike's PUA.

3 Mike's PUA responds to John's PUA that the call from John is accepted	Called Party Identity = Mike UCI <number>
	Calling Party Identity = John Fields UCI <label; number =withheld>
	Command = Accept Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Mike's Home Phone
		Mike's PUA confirms acceptance of the call request to John Field's PUA.

Flow	Parameters	Action

4 John's PUA instructs his SA to set up a call to Mike's Home Phone	Called Party Identity = Mike UCI <number>
	Calling Party Identity = John Fields UCI <label; number =withheld>
	Command = Establish Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Mike's Home Phone
		On receipt of the confirmation from Mike's PUA, John Field's PUA progresses with the call request to Mike by supplying the network with sufficient information to set up the call to Mike's Home Phone.

NOTE: A Call is set up from John's terminal to Mike's Home Phone. Mike recognizes his personal ringing tone on an incoming call and sees the name "John Fields" clearly shown on the telephone display - so he takes the call.		

Step 4 - Issues

- The distinctive ringing supplementary service has to be invoked (for Jenny and Mike's fixed telephony service) to associate different tones with calls to different UCIs.
- The name shown is the UCI label (which the PUA/network must be capable of delivering and the terminal must be capable of displaying).
- Provision for withholding or releasing the numeric (and other) elements of the UCI should be supported.

A.3.3.5 Step 5 - 'Old school friend' roams onto Home Phone

Next day John arrives at Mike and Jenny's and decides to stay overnight at short notice. He wants to call a few people to tell them what he's doing. John puts his Smart Card in the telephone's reader. His own address book is now available and he makes the required phone calls (including one using one of his "alias" identities).

This ensures that calls are booked to John's account, that John's PUA knows the identification of the terminal, that he has access to his own personal address book and that his UCI is given out as the originator of his communications. The use of the Smart Card permits a short-term override of the PUA defaults to be made without the user needing to manually change PUA preference settings.

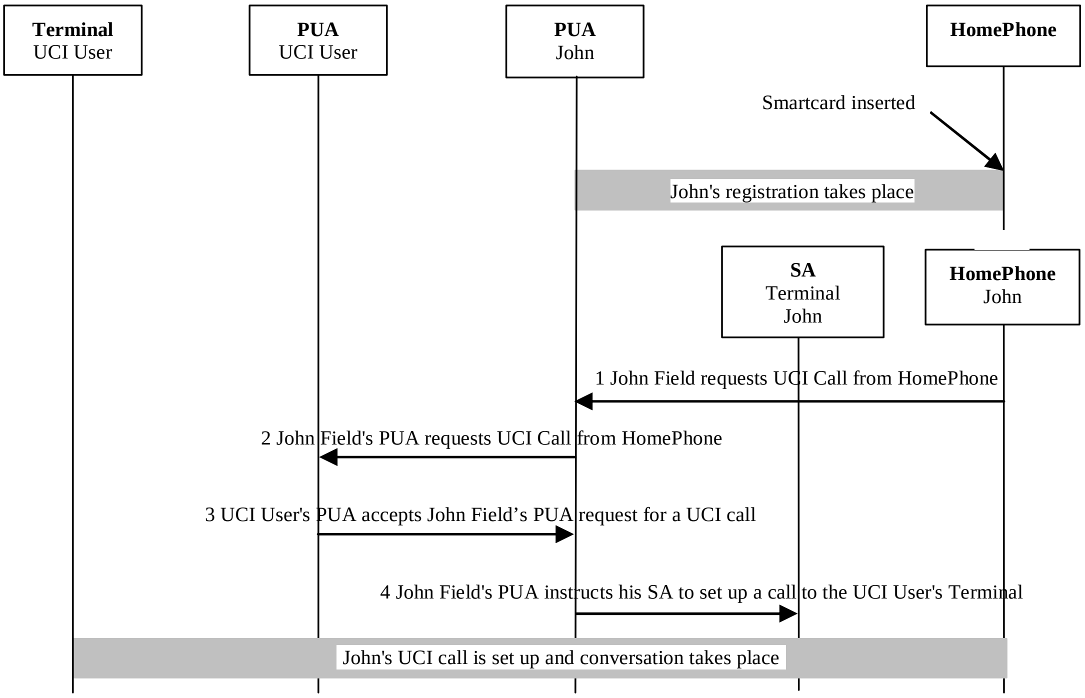

Terminal
UCI User
PUA
UCI User
PUA
John
HomePhone
Smartcard inserted
John's registration takes place
SA
Terminal
John
HomePhone
John
1 John Field requests UCI Call from HomePhone
2 John Field's PUA requests UCI Call from HomePhone
3 UCI User's PUA accepts John Field's PUA request for a UCI call
4 John Field's PUA instructs his SA to set up a call to the UCI User's Terminal
John's UCI call is set up and conversation takes place

Figure A.8: Home Scenario - Step 5 - 'Old school friend' roams onto Home Phone

Flow	Parameters	Action
Smartcard inserted into terminal reader The insertion of the smartcard initiates a registration procedure which makes contact with John's PUA and binds with the SA		
1 John Fields requests his PUA to set up a UCI call from the HomePhone	Called Party Identity = Any UCI <number> Calling Party Identity = John Fields UCI <label; number =withheld> Service Type = P-P real-time voice QoS = PSTN voice	John Fields initiates a call. It is assumed that John Fields has invoked the calling number restriction service.
2 John Smith's PUA informs UCI User's PUA of a new call	Called Party Identity = Anyother UCI <number> Calling Party Identity = John Field's UCI <label /alias; number =withheld> Command = Call Request Service Type = P-P real-time voice QoS = PSTN voice	John Field's PUA negotiates a new call using the calling name (alias) information stored in his profile.
3 UCI User's PUA responds to John's PUA that the call from John Smith is acceptable	Called Party Identity = Anyother UCI <number> Calling Party Identity = John Field's UCI <label /alias; number =withheld> Command = Accept Call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to UCI User's terminal	
4 John Field's PUA instructs John's SA to set up a call from his terminal to the UCI User's Terminal	Called Party Identity = Anyother UCI <number> Calling Party Identity = John Field's UCI <label /alias; number =withheld> Command = Establish Call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to UCI User's terminal	
Call set up from John's terminal to UCI User's terminal		

Step 5 - Issues

- The Terminal must support smartcard with automatic registration.
- The PUA supports calling name presentation (CNIP).

A.4 Tennis Club Scenario

A.4.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- the ability of one PUA to form an association with another PUA as a result of the individual having different roles associated with each PUA (Step 1);

- notification to the user that an incoming communication is associated with a specific role as it has been offered by the PUA assigned to that role (Steps 2 and 5);
- the ability of PUAs to associate, by default, one of the user's roles with an outgoing communication as a result of the previous communication being received in relation to that role (Step 3);
- user entry of the numeric element of a UCI taken from a business card and the user's ability to manually select one of their roles for outgoing communication (Step 4);
- a person who has no personal UCI, and hence no personal PUA, making outgoing UCI communications using the UCI supplied to him in relation to a role in an organization (Step 6).

A.4.2 Scenario description

The club PUA is a special case of the corporate PUA where PUAs representing club-role UCIs are "grouped". These role UCIs provide pointers either to an individual's specific terminals or to an individual's UCI. This scenario shows how such an arrangement facilitates the efficient running of a social club and how the privacy of individuals performing club roles is not compromised.

Table A.3: Tennis Club Scenario

Scenario Description	Technical Notes
STEP 1	
The Ipswich Tennis Club has invested in its own PUA to help manage its communications. Club Secretary Dennis has used the PUA Profile Management Application to define how communications are to be handled. He has assigned 10 people to the various club roles including Fred the membership secretary and Derek the treasurer.	A specialized application accessed via Dennis's PC facilitates setting up a Group PUA with routing tables and "fall-back" procedures related to each member of the group. Each club member will be assigned one of the UCIs that have been allocated the club.
As Fred and some of the other officials have their own PUAs, their incoming Tennis Club role communications will be offered directly to those people's PUAs. This involves Dennis in very little work as contact rules are already defined in the individual's PUA.	Dennis enters Fred's UCI in the routing table to ensure all Tennis Club Secretary communication requests are directed to Fred's PUA. Dennis does not need to enter any further information relating to Fred. In other cases people occupying club roles, such as Derek the treasurer, do not have their own PUAs and rules will have to be put into the club PUA. For instance Derek has told Dennis that any calls on a weekday (9 to 5) can go to his work number, evening calls to the club voicemail. This is more time-consuming for Dennis.
STEP 2	
New-to-the-area Paul wants to join the Club. He inputs "Ipswich Tennis Club" into his WAP-based directory search engine and receives ten hits back corresponding to the ten club roles. He selects "Membership Secretary" and clicks on "voice". Paul clicks on connect and a call is set up displaying Paul's name and the fact that it is Tennis Club business on Fred's terminal.	The search returns details of all the currently active UCIs allocated to the Tennis Club (in this case 10). When an officer of the club has their own PUA, the club PUA records the incoming communication request and forwards it to the individual's PUA. Those with Club UCIs must know when an incoming communication is club business. When the call arrives, Fred will be notified that the call has been delivered via the Tennis Club PUA (so that he knows that he should respond in his Tennis Club role). An entry for Paul will be made in the "Tennis Club" section of Fred's personal address book (if Fred wishes it to be added.

Scenario Description	Technical Notes
STEP 3 Fred calls Paul back to provide some extra information. Despite the fact that the call is made from Fred's home, the UCI label displayed on Paul's telephone display is "Membership Sec, Ipswich Tennis Club" and NOT Fred's personal UCI.	As Fred's personal PUA address book has already identified that Paul is associated with the Tennis Club, the Tennis Club Membership Secretary role is automatically selected. Thus, all Fred's communications to Paul will be passed through the Tennis Club PUA and labelled as "Membership Sec, Ipswich Tennis Club" by the Tennis Club PUA. The club PUA records all outgoing communication requests.
STEP 4 Fred now needs to email another prospective member, George, who gave him a business card a few days ago and is interested in joining the club. This time he has to select "Membership Secretary" to replace his name in the "from" field.	When making an outgoing communication to a new person, Fred will need to manually select the Tennis Club Secretary role as his PUA has no knowledge of the appropriate role for this particular communication.
STEP 5 A local shopkeeper wants to ask the club treasurer why a bill has not been paid and selects "Treasurer, Ipswich Tennis Club" from his mobile address book. This connects him to Derek's work telephone after Derek receives an indication telling him that this is a Tennis Club call.	In this instance, the club PUA must take on the routing/filtering functionality. The club PUA is aware that Derek does not have a personal PUA. The rules given to the club PUA mean that because this is a daytime call it will connect straight to Derek's work telephone. If Derek's work phone does not have a display, then the indication that the call is Tennis Club related has to be provided by some other means (e.g. voice announcement before the speech path is established).
STEP 6	
Derek has also been asked to contact George with details of club fees. To be identified in his club role and to ensure that the club is billed for the call, Derek has to dial a club account access number and put in his PIN. He is now able to enter George's UCI and will be identified by George as "club treasurer".	Derek is a non-PUA user who needs to take on the personality of the Tennis Club role he has been assigned when making an outgoing call. This means accessing the Tennis Club PUA and identifying himself in a similar manner to the procedures associated with current telephony charge-cards.

A.4.3 Discussion

A.4.3.1 Step 1 - Configuration Management

The Ipswich Tennis Club has invested in its own PUA to help manage its communications. Club Secretary Dennis has used the PUA Profile Management Application to define how communications are to be handled. He has assigned 10 people to the various club roles including Fred the membership secretary and Derek the treasurer.

A specialized application accessed via Dennis's PC facilitates setting up a Group PUA with routing tables and "fall-back" procedures related to each member of the group. Each club member will be assigned one of the UCIs that have been allocated the club.

As Fred and some of the other officials have their own PUAs, their incoming Tennis Club role communications will be offered directly to those people's PUAs. This involves Dennis in very little work as contact rules are already defined in the individual's PUA.

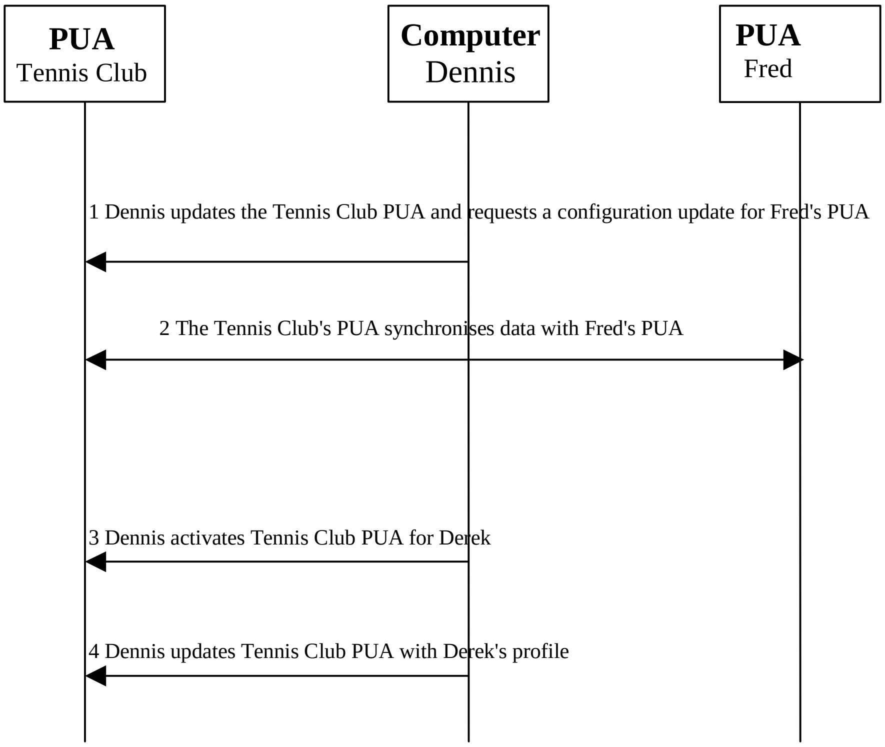

PUA
Tennis Club
Computer
Dennis
PUA
Fred
1 Dennis updates the Tennis Club PUA and requests a configuration update for Fred's PUA
2 The Tennis Club's PUA synchronises data with Fred's PUA
3 Dennis activates Tennis Club PUA for Derek
4 Dennis updates Tennis Club PUA with Derek's profile

Figure A.9: Tennis Club - Step 1 - Configuration management

Flow	Parameters	Action

1 Dennis updates Tennis Club PUA with Fred's PUA address	User identity = Dennis's UCI
	Command = Add
	Destination = Tennis Club PUA
	Item = Fred's UCI; Routing Table - Secretary entry
		Dennis enters data on Fred's UCI in the routing table to ensure all Tennis Club Secretary communication requests are directed to Fred's PUA. Dennis does not need to enter any further information relating to Fred.

2 The Tennis Club's PUA synchronizes data with Fred's PUA	Command = Synchronize
	Source = Tennis Club PUA
	Destination = Fred's PUA
	Item = Fred's UCI; Routing Table	

3 Dennis activates Tennis Club PUA for Derek	User identity = Dennis' UCI
	Command = Add
	Source = Tennis Club PUA
	Item = Derek's contact details; Routing Table-Treasurer entry
		Dennis enters Derek the treasurer's details.

4 Dennis updates Tennis Club PUA with Derek's profile	User identity = Dennis' UCI
	Command = Add
	Source = Tennis Club PUA
	Item = Derek's contact rules; Rule Table-Treasurer entry
		Derek does not have his own PUA. The necessary rules will have to be entered into the club PUA. For instance Derek has told Dennis that any calls on a weekday (9 to 5) can go to his work number, evening calls to the club voicemail.

NOTE: Ditto for each Tennis Club officer.		

Step 1 - Issues

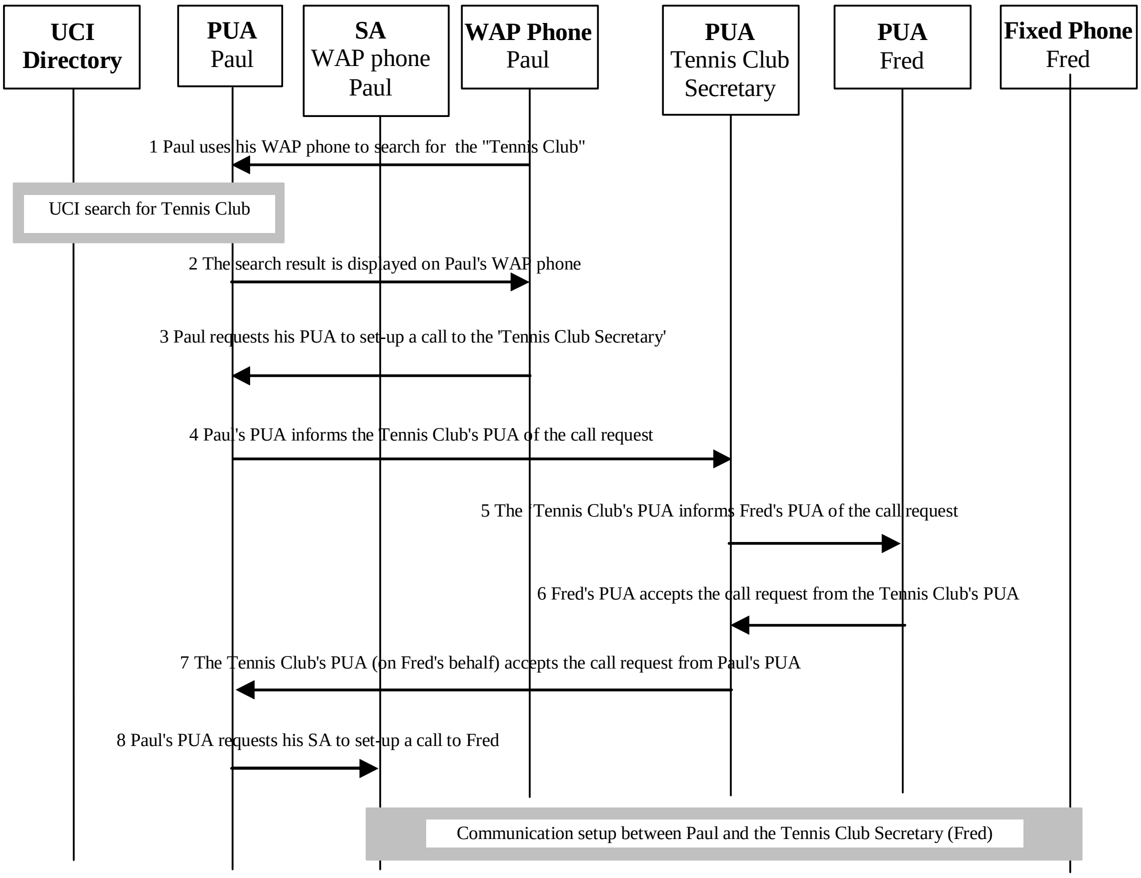
- The ability to perform configuration management on the Tennis Club PUA must be supported

A.4.3.2 Step 2 - Club membership enquiry

New-to-the-area Paul wants to join the Club. He inputs "Ipswich Tennis Club" into his WAP-based directory search. The search returns details of all the currently active UCIs allocated to the Tennis Club (in this case 10). Paul selects "Membership Secretary" and "voice". He clicks on connect and a call is set up displaying Paul's name and the fact that it is Tennis Club business on Fred's terminal.

When an officer of the club has their own PUA, the club PUA records the incoming communication request and forwards it to the individual's PUA. Those with Club UCIs must know when an incoming communication is club business.

When the call arrives, Fred will be notified that the call has been delivered via the Tennis Club PUA (so that he knows that he should respond in his Tennis Club role). An entry for Paul will automatically be made in the "Tennis Club" section of Fred's personal address book.



UCI Directory
PUA Paul
SA WAP phone Paul
WAP Phone Paul
PUA Tennis Club Secretary
PUA Fred
Fixed Phone Fred
1 Paul uses his WAP phone to search for the "Tennis Club"
UCI search for Tennis Club
2 The search result is displayed on Paul's WAP phone
3 Paul requests his PUA to set-up a call to the 'Tennis Club Secretary'
4 Paul's PUA informs the Tennis Club's PUA of the call request
5 The Tennis Club's PUA informs Fred's PUA of the call request
6 Fred's PUA accepts the call request from the Tennis Club's PUA
7 The Tennis Club's PUA (on Fred's behalf) accepts the call request from Paul's PUA
8 Paul's PUA requests his SA to set-up a call to Fred
Communication setup between Paul and the Tennis Club Secretary (Fred)

Figure A.10: Tennis Club - Step 2 -Club membership enquiry

Flow	Parameters	Action

1 Paul uses his WAP phone to search for the 'Tennis Club'	User identity = Paul UCI
	Command = Search
	Source = UCI database
	Search parameters = 'Ipswich Tennis Club'
		Paul requests contact details of the 'Ipswich Tennis Club'. This could be a proprietary www-based application.

Paul searches for details of the Ipswich Tennis Club UCIs		

2 The search result is displayed on Paul's WAP phone	User identity = Paul's PUA
	Command = Results
	Sourceref = UCI database
	Item = List of all (10) publicly available Tennis Club UCIs
		The search application returns via the PUA, the stored contact details of all the currently active UCIs allocated to the Tennis Club (in this case 10).

3 Paul requests his PUA to set-up a call to the 'Tennis Club Secretary'	Called party Identity = Tennis Club Secretary UCI <number> Calling Party identity = Paul UCI <label; number> Service Type = P-P real-time voice QoS = PSTN voice	Paul selects "Membership Secretary" and "voice". He clicks on connect and a call set-up request is sent to the Tennis Club Secretary PUA.
4 Paul's PUA informs the Tennis Club's PUA of the call request	Called party Identity = Tennis Club Secretary UCI <number> Calling Party identity = Paul UCI <label; number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	Paul's PUA receives the set-up request for a call to the tennis club secretary and sends a call indication to the tennis club secretary's PUA.
5 The 'Tennis Club's PUA informs the Fred's PUA of the call request	Called party Identity = Tennis Club Secretary UCI <number> Calling Party identity = Paul UCI <label; number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	The call request arrives at the PUA for the tennis club secretary. Since Fred is an officer of the club and has his own PUA, the club PUA records the incoming communication request and forwards it to the Fred's PUA.

6 Fred's PUA accepts the call request from the Tennis club's PUA	Called party Identity = Tennis Club Secretary UCI <number>
	Calling Party identity = Paul UCI <label; number>
	Command =Accept Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Fred's Home Phone
		The call indication arrives at Fred's PUA which accepts the call and returns to the Tennis Club Secretary's PUA details to set-up a call to Fred's fixed phone.

7 The Tennis Club's PUA (on Fred's behalf) accepts the call request from Paul's PUA	Called party Identity = Tennis Club Secretary UCI <number>
	Calling Party identity = Paul UCI <label; number>
	Command = Accept Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Fred's Home Phone
		The Tennis Club Secretary's PUA supplies data to Paul's PUA to redirect the call to Fred's fixed phone. An authentic called party identity indication of ***"Tennis Club - Secretary"*** is available for display on Paul's terminal.

8 Paul's PUA instructs his SA to set up a call to Fred's Home Phone	Called party Identity = Tennis Club Secretary UCI <number>
	Calling Party identity = Paul UCI <label; number>
	Command = Establish Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Fred's Home Phone
		On receipt of the confirmation from the Tennis Club Secretary's PUA, Paul's PUA progresses with the call request by supplying the network with sufficient information to set up the call to Fred's Home Phone.

NOTE: A call is established between Paul and the "Tennis Club - Secretary" on Fred's home phone.		

Step 2 - Issues

- The UCI directory search returns all active UCIs for the tennis club.
- The tennis club secretary's PUA records incoming communication requests.
- The tennis club secretary's PUA forwards the call indication to Fred's PUA.
- The Calling Party Identity 'Tennis Club - Secretary' is returned to the caller even though the call is eventually delivered to Fred.

A.4.3.3 Step 3 - Response to club membership enquiry

Fred calls Paul back to provide some extra information. Despite the fact that the call is made from Fred's home, the UCI label displayed on Paul's telephone display is "Membership Sec, Ipswich Tennis Club" and NOT Fred's personal UCI.

As Fred's personal PUA address book has already identified that Paul is associated with the Tennis Club, the Tennis Club Membership Secretary role is automatically selected. Thus, all Fred's communications to Paul will be passed through the Tennis Club PUA and labelled as "Membership Sec, Ipswich Tennis Club" by the Tennis Club PUA. The club PUA records all outgoing communication requests.

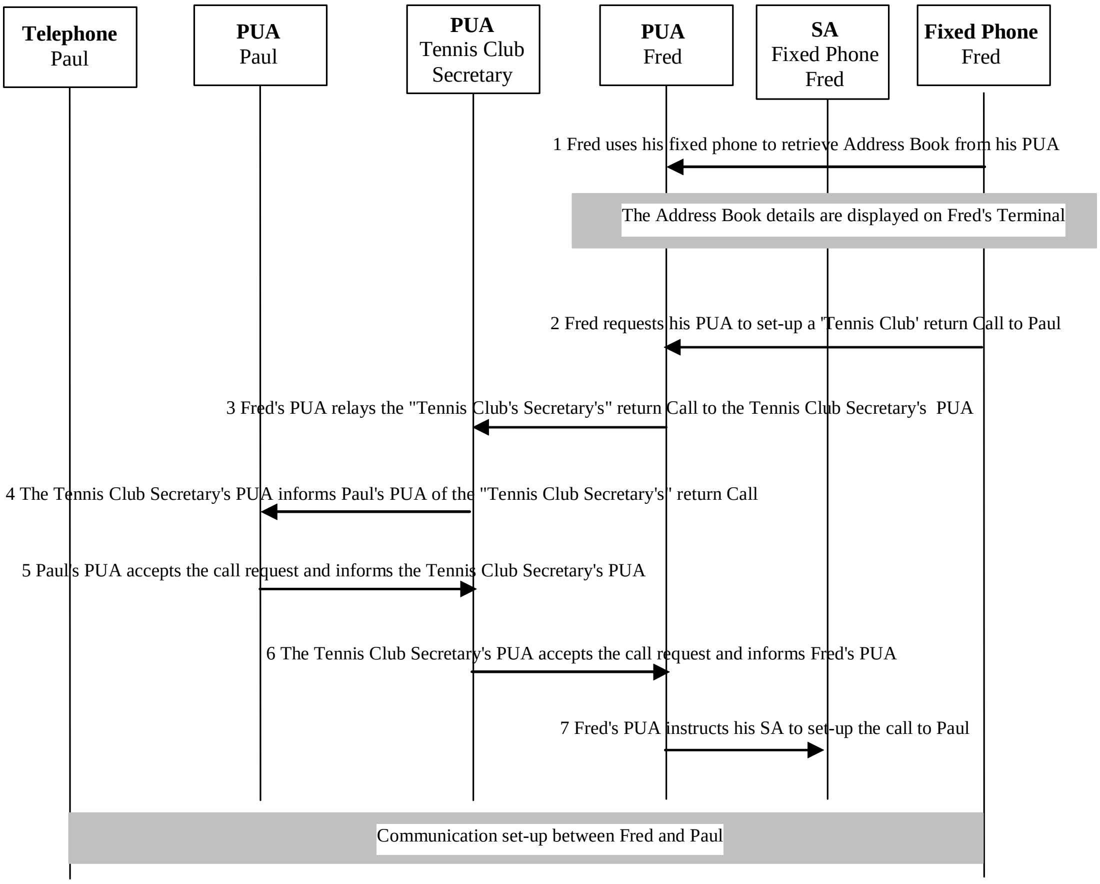

Telephone Paul
PUA Paul
PUA Tennis Club Secretary
PUA Fred
SA Fixed Phone Fred
Fixed Phone Fred
1 Fred uses his fixed phone to retrieve Address Book from his PUA
The Address Book details are displayed on Fred's Terminal
2 Fred requests his PUA to set-up a 'Tennis Club' return Call to Paul
3 Fred's PUA relays the "Tennis Club's Secretary's" return Call to the Tennis Club Secretary's PUA
4 The Tennis Club Secretary's PUA informs Paul's PUA of the "Tennis Club Secretary's" return Call
5 Paul's PUA accepts the call request and informs the Tennis Club Secretary's PUA
6 The Tennis Club Secretary's PUA accepts the call request and informs Fred's PUA
7 Fred's PUA instructs his SA to set-up the call to Paul
Communication set-up between Fred and Paul

Figure A.11: Tennis Club - Step 3 - Response to club membership enquiry

Flow	Parameters	Action

1 Fred uses his fixed phone to retrieve his Address Book from his PUA	User identity = Fred UCI
	Command = Get
	Source = Fred's PUA
	Item = Address Book
	Authentication =
		Fred retrieves his address book from his PUA so that it can be viewed according to criteria such as date ranges and contact names (UCI Labels).

Fred reads his address book and selects the "Tennis Club - Secretary" for a return call		
2 Fred requests his PUA to set-up a 'Tennis Club' return call to Paul	Called Party Identity = Paul UCI <number> Calling Party Identity = Tennis Club Secretary UCI < label, number> Service Type = P-P real-time voice QoS = PSTN voice	As Paul's entry in Fred's address book marks him as related to Tennis Club business, Fred's PUA offers the "membership secretary, Ipswich Tennis Club" role as the default option for returned communications originating from the tennis club PUA.
3 Fred's PUA relays to the Tennis Club Secretary's PUA the Tennis Club Secretary's return call	Called Party Identity = Paul UCI <number> Calling Party Identity = Tennis Club Secretary UCI < label, number> Command =Call request Service Type = P-P real-time voice QoS = PSTN voice	The returned communications would be labelled as "membership secretary, Ipswich Tennis Club" and not "Fred" (his own name).
4 The Tennis Club Secretary's PUA informs Paul's PUA of the Tennis Club Secretary's return call	Called Party Identity = Paul UCI <number> Calling Party Identity = Tennis Club Secretary UCI < label, number> Command =Call request Service Type = P-P real-time voice QoS = PSTN voice	Fred's communications to Paul has been passed through the Tennis Club Secretary PUA and labelled as "Membership Sec, Ipswich Tennis Club" by the Tennis Club PUA. The club PUA records all outgoing communication requests and extends the request to Paul's PUA.
5 Paul's PUA accepts the call request and informs the Tennis Club Secretary's PUA	Called Party Identity = Paul UCI <number> Calling Party Identity = Tennis Club Secretary UCI < label, number> Command =Accept Call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to Paul's telephone	The call set-up is accepted and relayed back to the originator.
6 The Tennis Club Secretary's PUA accepts the call request and informs Fred's PUA	Called Party Identity = Paul UCI <number> Calling Party Identity = Tennis Club Secretary UCI < label, number> Command =Accept Call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to Paul's telephone	The call set-up is accepted and relayed back to the originator.
7 Fred's PUA instructs his SA to set-up the call to Paul	Called Party Identity = Paul UCI <lnumber> Calling Party Identity = Tennis Club Secretary UCI < label, number> Command =Establish Call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to Paul's telephone	Fred's SA instructs the network to set-up the call using normal call set-up procedures.
NOTE: The return call is established without revealing Fred's personal identity.		

Step 3 - Issues

- The tennis club PUA must record outgoing communication requests.
- The tennis club PUA must populate the Calling Party Identity fields with the appropriate data for the Ipswich Tennis Club - Membership Secretary's Role.

A.4.3.4 Step 4 - Further club membership enquiry

Fred now needs to email another prospective member, George, who gave him a business card a few days ago and is interested in joining the club. This time he has to select "Membership Secretary" to replace his name in the "from" field.

When making an outgoing communication to a new person, Fred will need to manually select the Tennis Club Secretary role as his PUA has no knowledge of the appropriate role for this particular communication.

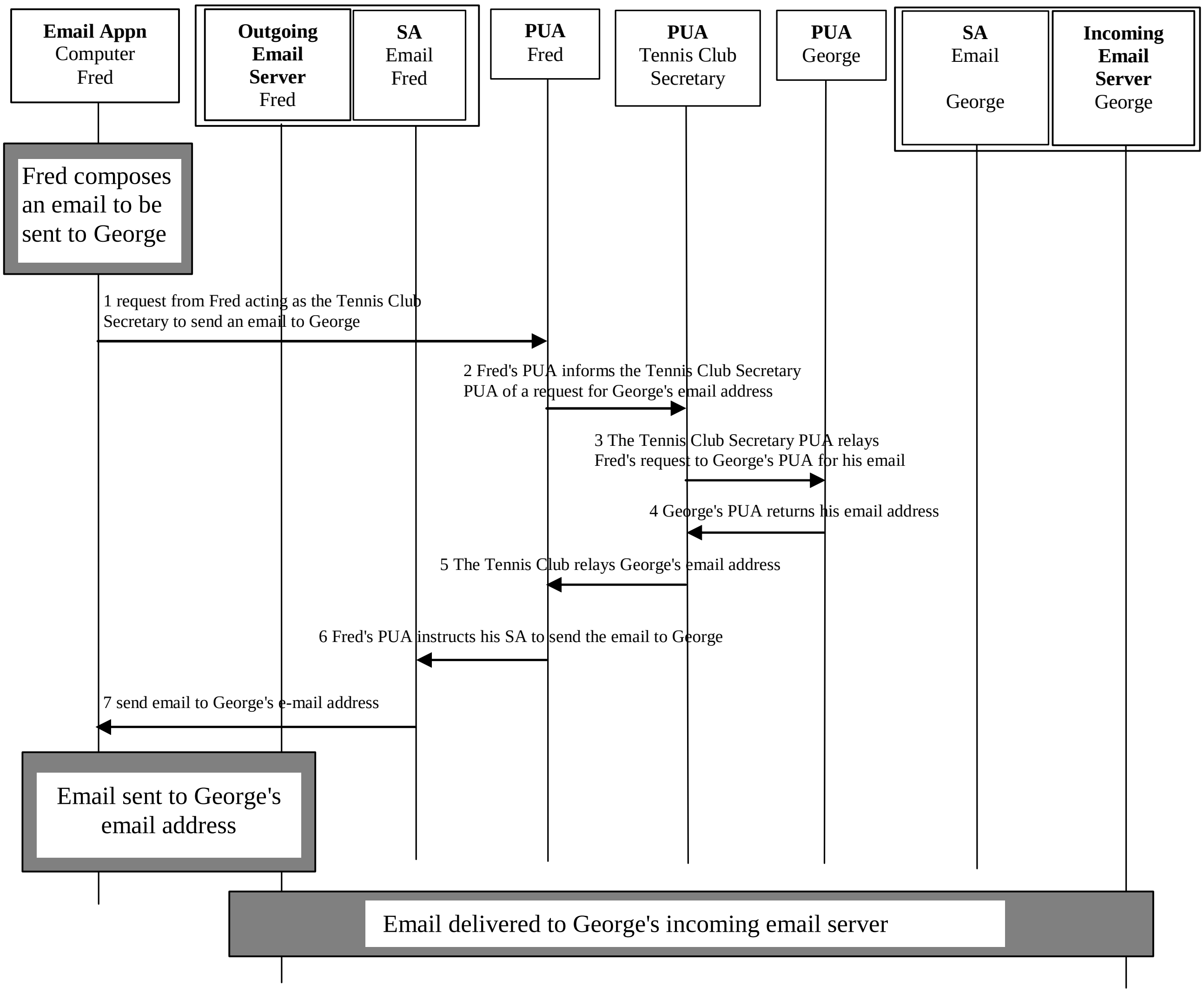

Email Appn Computer Fred
Outgoing Email Server Fred
SA Email Fred
PUA Fred
PUA Tennis Club Secretary
PUA George
SA Email George
Incoming Email Server George
Fred composes an email to be sent to George
1 request from Fred acting as the Tennis Club Secretary to send an email to George
2 Fred's PUA informs the Tennis Club Secretary PUA of a request for George's email address
3 The Tennis Club Secretary PUA relays Fred's request to George's PUA for his email
4 George's PUA returns his email address
5 The Tennis Club relays George's email address
6 Fred's PUA instructs his SA to send the email to George
7 send email to George's e-mail address
Email sent to George's email address
Email delivered to George's incoming email server

Figure A.12: Tennis Club - Step 4 - Further club membership enquiry

Flow	Parameters	Action
Fred composes an email to be sent to George		

1 Request from Fred acting as the Tennis Club secretary to send an email to George	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Request Data
	Item = sendto email address
		Fred composes his e-mail to George. Fred selects the "membership secretary, Ipswich Tennis Club" role and enters the numeric part of George's email (which is shown on George's business card). The selecting of the "membership secretary, Ipswich Tennis Club" role determines that the communication request is routed to the Tennis Club Secretary PUA.

2 Fred's PUA informs the Tennis Club PUA of a request for George's Email address	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Request Data
	Item = sendto email address
		The communication will be labelled as "membership secretary, Ipswich Tennis Club" and not "Fred" (his own name).

3 The Tennis Club Secretary's PUA relays Fred's request for his email address to George's PUA	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Request Data
	Item = sendto email address
		The request for George's email address is relayed to Georges PUA. Fred's email request to George has been passed through the Tennis Club PUA and labelled as "Membership Sec, Ipswich Tennis Club" by the Tennis Club PUA. The club PUA records all outgoing communication requests.

4 Georges PUA returns his email address to the Tennis Club Secretary's PUA	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Data Supplied
	Item = sendto email address	

5 Tennis Club Secretary's PUA relays the returned address to Fred's PUA	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Data Supplied
	Item = sendto email address	

6 Fred's PUA instructs his SA to send the Email communication to Fred's email application	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Data Supplied
	Item = sendto email address	

7 Fred's SA requests the email application to send the email to George's address	Called Party Identity = George UCI <number>
	Calling Party Identity = Tennis Club Secretary UCI < label, number>
	Command = Send mail to
	Item = sendto email address	

Step 4 - Issues

- The tennis club PUA must record outgoing communication requests (including e-mail).

- The tennis club PUA must populate the Calling Party Identity 'e-mail' fields with the appropriate data for the Ipswich Tennis Club - Membership Secretary's Role.

A.4.3.5 Step 5 - Communication for the Club Treasurer

A local shopkeeper wants to ask the club treasurer why a bill has not been paid and selects "Treasurer, Ipswich Tennis Club" from his mobile address book. In this instance, the club PUA must take on the routing/filtering functionality.

The club PUA is aware that the Treasurer, Derek, does not have a personal PUA. The rules given to the club PUA mean that because this is a daytime call it will connect straight to Derek's work telephone. If Derek's work phone does not have a display, then the indication that the call is Tennis Club related has to be provided by some other means (e.g. voice announcement before the speech path is established).

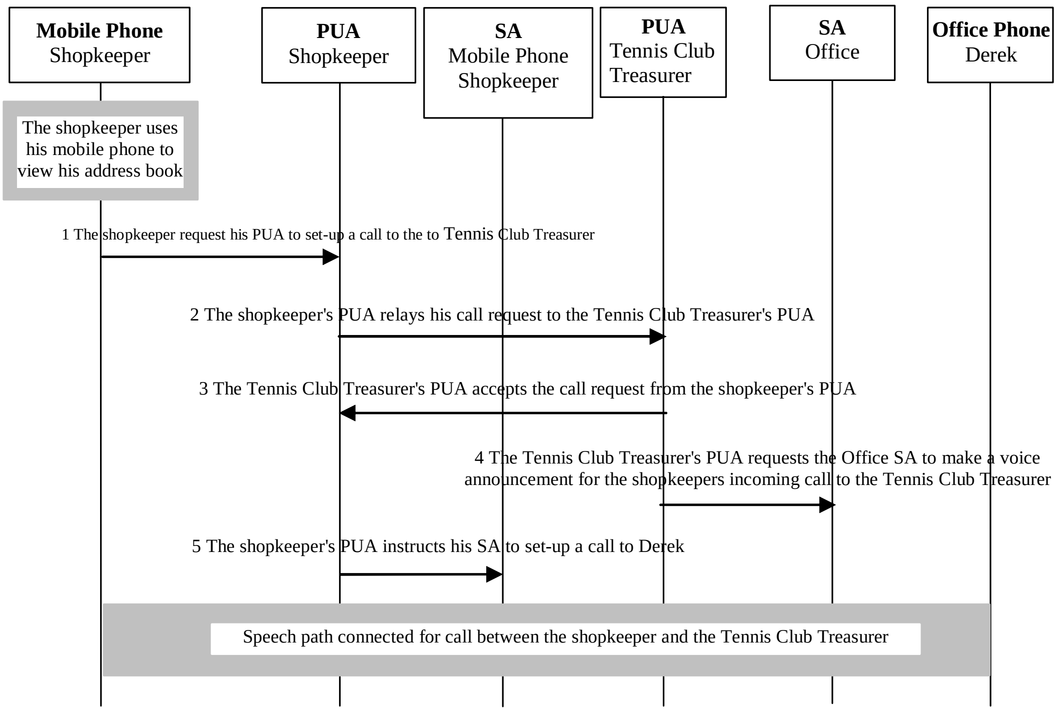

Mobile Phone
Shopkeeper
PUA
Shopkeeper
SA
Mobile Phone
Shopkeeper
PUA
Tennis Club
Treasurer
SA
Office
Office Phone
Derek
The shopkeeper uses his mobile phone to view his address book
1 The shopkeeper request his PUA to set-up a call to the to Tennis Club Treasurer
2 The shopkeeper's PUA relays his call request to the Tennis Club Treasurer's PUA
3 The Tennis Club Treasurer's PUA accepts the call request from the shopkeeper's PUA
4 The Tennis Club Treasurer's PUA requests the Office SA to make a voice announcement for the shopkeepers incoming call to the Tennis Club Treasurer
5 The shopkeeper's PUA instructs his SA to set-up a call to Derek
Speech path connected for call between the shopkeeper and the Tennis Club Treasurer

Figure A.13: Tennis Club - Step 5 - Communication for the Club Treasurer

Flow	Parameters	Action
Shopkeeper views the address book stored in the mobile phone and selects Tennis Club Treasurer.		
1 The shopkeeper requests his PUA to set-up a call to 'Tennis Club Treasurer.	Called Party Identity = Tennis Club Treasurer UCI <numeric> Calling Party Identity = Shopkeeper UCI <label; numeric> Service Type = P-P real-time voice QoS = PSTN voice	The shopkeeper selects the Treasurer for the Ipswich tennis Club from his 'mobile' address book and sends a call set-up request to his PUA.
2 The shopkeeper's PUA relays the call set-up request to the Tennis Club Treasurer's PUA	Called Party Identity = Tennis Club Treasurer UCI < numeric> Calling Party Identity = Shopkeeper UCI <label; numeric> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	The shopkeeper's PUA processes the call set-up request constructed on the shopkeeper's mobile terminal by providing the calling party identity information and routes the request to the Tennis Club Treasurer's PUA.
3 The 'Tennis Club Treasurer's PUA accepts the call set-up request from the Shopkeeper's PUA.	Called Party Identity = Tennis Club Treasurer UCI <numeric> Calling Party Identity = Shopkeeper UCI <label; numeric> Command = Accept call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to Derek's office phone	The Tennis Club's PUA accepts the call fro the shopkeeper and records the incoming call request. The PUA is aware that Derek does not have a personal PUA but that the rules given to the club PUA mean that because this is a daytime call it will connect straight to Derek's work telephone.

4 The Tennis Club's PUA requests the Office SA to make a voice announcement for the shopkeeper's incoming call to the Tennis Club's Treasurer.	Called Party Identity = Tennis Club Treasurer UCI <numeric>
	Calling Party Identity = Shopkeeper UCI <label; numeric>
	Command = Announce incoming call
	Data = Shopkeeper UCI <label>
	Service Type = P-P real-time voice
	QoS = PSTN voice
		The PUA routes the call set-up request to the SA for Derek's office phone and make a voice announcement. Even though Derek does not have a UCI, a default SA associated with the network to which Derek's Office is connected will always be assigned to handle UCI related requests.

5 The shopkeeper's PUA instructs his SA to set-up a call to Derek	Called Party Identity = Tennis Club Treasurer UCI <numeric> Calling Party Identity = Shopkeeper UCI <label; numeric> Command = Establish call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to Derek's office phone	The shopkeeper's PUA asks his SA to establish the call to Derek.
NOTE: Following the voice announcement, a two-way speech path is connected between the shopkeeper and Derek's office phone.		

Step 5 - Issues

- The tennis club's PUA retains the calling and called party identities when delivering the call to Derek's office phone.
- The tennis club's PUA knows the capabilities of Derek's office terminal and has to play an announcement prior to completing the speech path to the calling party.
- A default SA associated with a network or service will always be assigned to handle UCI related communications associated with calls to a subscriber to that network or service.

A.4.3.6 Step 6 - Non-PUA User makes Tennis Club call

Derek has also been asked to contact George with details of club fees. To be identified in his club role and to ensure that the club is billed for the call, Derek has to dial a club account access number and put in his PIN. He is now able to enter George's UCI and will be identified by George as "club treasurer".

Derek is a non-PUA user who needs to take on the personality of the Tennis Club role he has been assigned when making an outgoing call. This means accessing the Tennis Club PUA and identifying himself in a similar manner to the procedures associated with current telephony charge-cards.

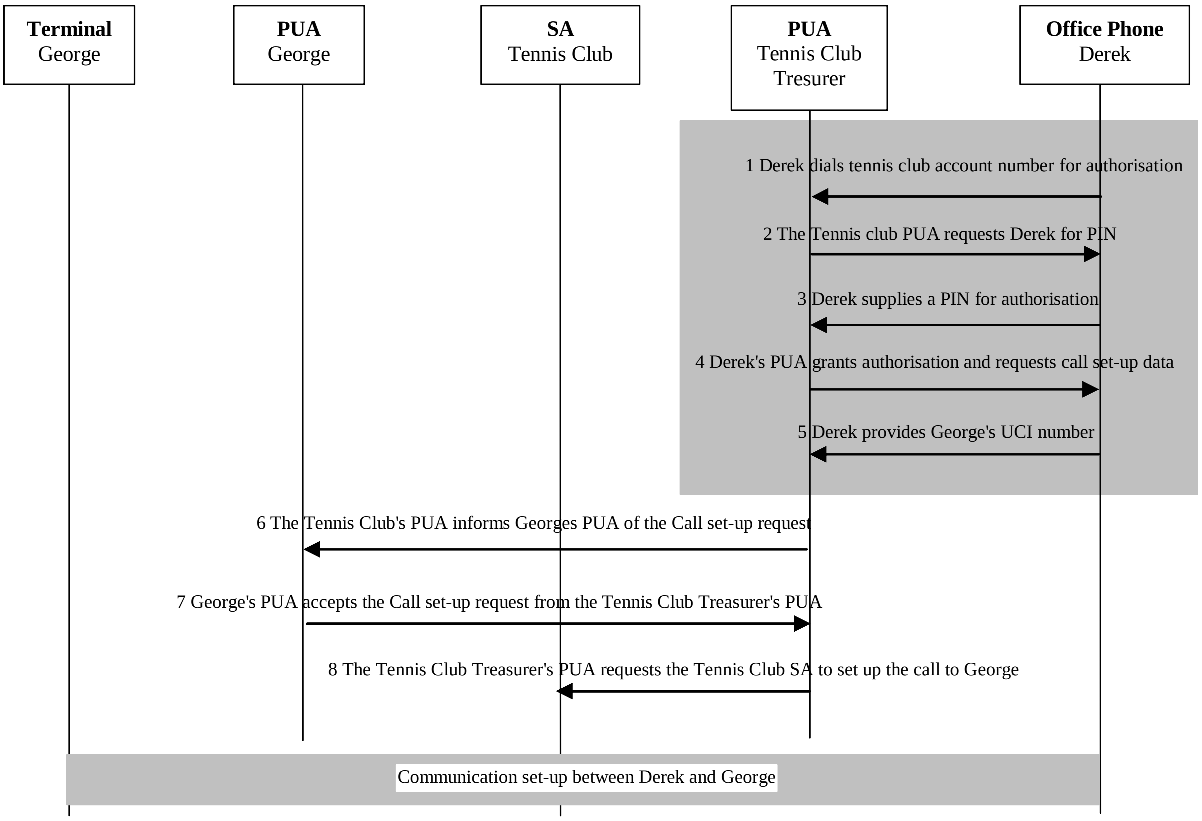

Terminal
George
PUA
George
SA
Tennis Club
PUA
Tennis Club
Tresurer
Office Phone
Derek
1 Derek dials tennis club account number for authorisation
2 The Tennis club PUA requests Derek for PIN
3 Derek supplies a PIN for authorisation
4 Derek's PUA grants authorisation and requests call set-up data
5 Derek provides George's UCI number
6 The Tennis Club's PUA informs Georges PUA of the Call set-up request
7 George's PUA accepts the Call set-up request from the Tennis Club Treasurer's PUA
8 The Tennis Club Treasurer's PUA requests the Tennis Club SA to set up the call to George
Communication set-up between Derek and George

Figure A.14: Tennis Club - Step 6 - Non-PUA User makes Tennis Club call

Flow	Parameters	Action
1 Derek dials tennis club account number	Called party identity <number>	Derek makes a call to the tennis club account access number to be identified in his club role and to ensure that the club is billed for the call. The local network adds the calling party identity and establishes a call to the tennis club access account number.

2 The tennis club requests Derek for a PIN	Command = Enter UCI <numeric>
	Command = Enter PIN
		The tennis club requests the calling party to enter his UCI number and a PIN.

3 Derek supplies his PIN for authorization	Data = Treasurer UCI <numeric>
	Data = PIN
		Derek enters his UCI number and PIN.

4 The tennis club PUA grants authorization and requests call set-up data	Response = Authorized
	Command = Enter UCI number
		Derek is authorized to make outgoing calls on behalf of the tennis club and requested to dial the UCI number.

5 Derek provides George's UCI number	Called party identity = George's UCI <number>	Derek keys in Georges UCI for an outgoing call request.
6 The Tennis Club Treasurer PUA informs George's PUA of the call set-up request	Called party identity = George's UCI <number> Calling party identity = Tennis Club Treasurer UCI <label; number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	The tennis club PUA logs the call request, supplies the Calling Party Identity information and routes the call set-up request to Georges PUA.
7 George's PUA accepts the call set-up request from the Tennis Club PUA	Called party identity = George's UCI <number> Calling party identity = Tennis Club Treasurer UCI <label; number> Command = Accept call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to George's office phone	Georges PUA accepts the call request.
8 The Tennis Club PUA requests its SA to set-up the call to George	Called party identity = George's UCI <number> Calling party identity = Tennis Club Treasurer UCI <label; number> Command = Establish call Service Type = P-P real-time voice QoS = PSTN voice Data = Routing information for connecting call to George's office phone	The Tennis Club Treasurer's PUA requests its SA to set up the call to George.
NOTE: Communication set up between Derek and George.		

Step 6 - Issues

- The tennis club must have an application to support non-PUA owners who have "officer" roles in the club.
- The tennis club PUA must have a secure means to authenticate non-PUA users.

The tennis club PUA must log outgoing call requests.

A.5 Multiple Role Scenario

A.5.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- the way in which profile synchronization between PUAs associated with different roles can enable a communication associated with one role to be delivered to a terminal supplied by the organization associated with another role (Steps 1 and 2);
- the way in which the PUA can use the UCI from a record in the PUA's communication history in the set-up of a subsequent communication using the same or different type of communication service (Step 3);
- the way in which a PUA can assign a default outgoing UCI identity based upon the UCI that was used to contact the user, and that is now stored in the communication history (Step 3).

A.5.2 Scenario description

In many circumstances, individuals could be dependent on the communication rules embedded in two or more PUAs each relating to a different environment. It would appear sensible and efficient for those PUAs to share information related to an individual but there are obvious implications for security and privacy. This scenario shows how such an arrangement would appear to a user and what privacy/security capabilities would need to be put in place.

In this scenario, the character John Smith has had his own personal UCI for three years. He retired from full time work with Nokia five years ago but now his schedule is just as busy:

- On Tuesdays he does one days consultancy work on a regular basis for systems integration company SmartSys. They have supplied him with a permanently allocated desk on which is a telephone and PC, and provided him with a corporate UCI.
- He works intermittently throughout the year for ETSI, sometimes at home using his own communications equipment and sometimes in Sophia Antipolis where a telephone and PC are supplied plus a corporate UCI.
- He has just been elected a City Councillor in his spare time and the Council have now put an ISDN terminal in his house, loaned him a fax machine and supplied a corporate UCI.
- As if that isn't enough he is membership secretary for the local engineering club. They do not supply any communications equipment or services but forward communications to him when appropriate from a club UCI.

Table A.4: Multiple Workplace Scenario

Scenario Description	Technical Notes
BACKGROUND	
Besides his own personal PUA/UCI, John's communications are under the control of four other PUAs. John was initially worried that this seemingly complex communications environment would need very high maintenance. For instance he wondered if he would need to tell all the PUAs every time he went away for a few days.	When the council set up his corporate UCI they asked for details of his personal UCI and permission for the two associated PUAs to exchange information. The Council's PUA then set up a relationship with John's personal PUA. The individual's PUA will now inform the Council's PUA (and vice versa) of major changes such as a provision of a new service, or the non availability of the UCI owner.
John has discovered that this has not been the case.	Similar arrangements were made by the owners of the other PUAs.
STEP 1,2	
John has requested and now been allocated a mobile phone by SmartSys which he has been told he can also use for non SmartSys calls. The first evening that he has the mobile phone it rings while he is out working in the garden. A voice announcement tells him that the call has been forwarded from the engineering club and then connects him. It is a prospective member for the engineering club. John is impressed; somehow the club PUA is aware of and routed a call to his new mobile. John promises to call back the enquirer as soon as he returns to his house and has access to the club details on his PC.	The SmartSys PUA informs John's PUA that a mobile is now available and that SmartSys is happy for it also to receive non SmartSys calls. At the earliest opportunity John's personal PUA will ask him if he wishes to define additional contact rules relating to the mobile. In the meantime, as a default, it assumes that if the mobile is turned on then John is available for calls that are acceptable (as defined in his user profile). The caller sees only the club UCI as the recipient because the clubs PUA is the recipient as far as the originator is concerned.
STEP 3	
Back in the house John turns on his PC, opens his PUA Profile Management application and requests communications history details. The call requesting membership details is at the top of the list, being the latest communication. John clicks on this and then selects "return" and "voice call" and accepts the default role offered - "membership secretary, engineering club".	John's PUA knows that this call was forwarded from the engineering club PUA. The PUA would offer the "membership secretary, engineering club" role as the default option for returned communications originating from the engineering club PUA. The returned communications would be labelled as "membership secretary, engineering club" and not "John Smith" (his own name). Alternatively, John could have selected "John Smith" which would have passed on his personal UCI rather than the club one.
The call is established and John can now pass over the details on annual fees from his club database.	

A.5.3 Discussion

A.5.3.1 Step 1 - Configuration Management

John Smith has had his own personal UCI for three years. He retired from full time work with Nokia five years ago but now has just as busy a schedule however.

- On Tuesdays he does one day consultancy work on a regular basis for systems integration company SmartSys. They have supplied him with a permanently allocated desk on which is a telephone and PC, and provided him with a corporate UCI.
- He works intermittently throughout the year for ETSI, sometimes at home using his own communications equipment and sometimes in Sophia Antipolis where a telephone and PC are supplied plus a corporate UCI.
- He has just been elected a City Councillor in his spare time and the Council have now put an ISDN terminal in his house, loaned him a fax machine and supplied a corporate UCI.

- As if that is not enough he is membership secretary for the local engineering club. They do not supply any communications equipment or services but forward communications to him when appropriate from a club UCI.

So besides his own personal PUA/UCI John's communications are under the control of four other PUAs. John was initially worried that this seemingly complex communications environment would need very high maintenance. For instance he wondered if he would need to tell all the PUAs every time he went away for a few days.

When the council set up his corporate UCI they asked for details of his personal UCI and permission for the two associated PUAs to exchange information. The Council's PUA then set up a relationship with John's personal PUA. The individual's PUA will now inform the Council's PUA (and vice versa) of major changes such as a provision of a new terminal or service, or the non-availability of the UCI owner. The owners of the other PUAs made similar arrangements.

John has requested and now been allocated a mobile phone by SmartSys.

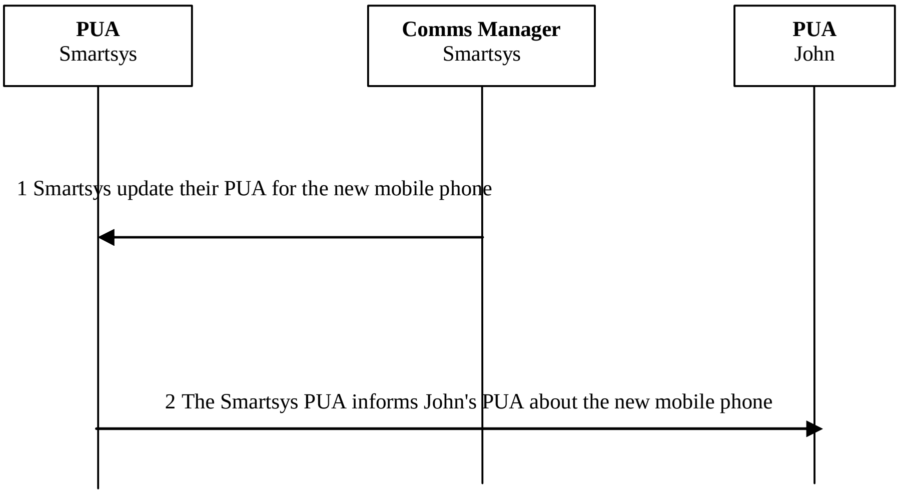

PUA
Smartsys
Comms Manager
Smartsys
PUA
John
1 Smartsys update their PUA for the new mobile phone
2 The Smartsys PUA informs John's PUA about the new mobile phone

Figure A.15: Multiple workplace - Step 1 - Configuration Management

Flow	Parameters	Action

1 Smartsys supplies a configuration update for John's PUA	User Identity = Communications Manager Smartsys UCI
	Command = Add
	Destination = John@Smartsys
	Item = Terminal id for mobile phone
		The Smartsys Communications manager enters John's new mobile phone into John's Smartsys PUA profile.

2 Smartsys PUA synchronizes data with John's PUA	User identity = John UCI
	Command = Add
	Source = John@Smartsys
	Item = Terminal id for mobile phone
		John's PUA receives the new terminal id data from the Smartsys PUA.

A.5.3.2 Step 2 - Inbound Engineering Club Communication

John has requested and now been allocated a mobile phone by Smartsys. The first evening that he has the mobile phone it rings while he is out working in the garden. A voice announcement tells him that the call has been forwarded from the engineering club and then connects him. It is a prospective member for the engineering club. John is impressed; somehow the club PUA is aware of and routed a call to his new mobile. John promises to call back the enquirer as soon as he returns to his house and has access to the club details on his PC.

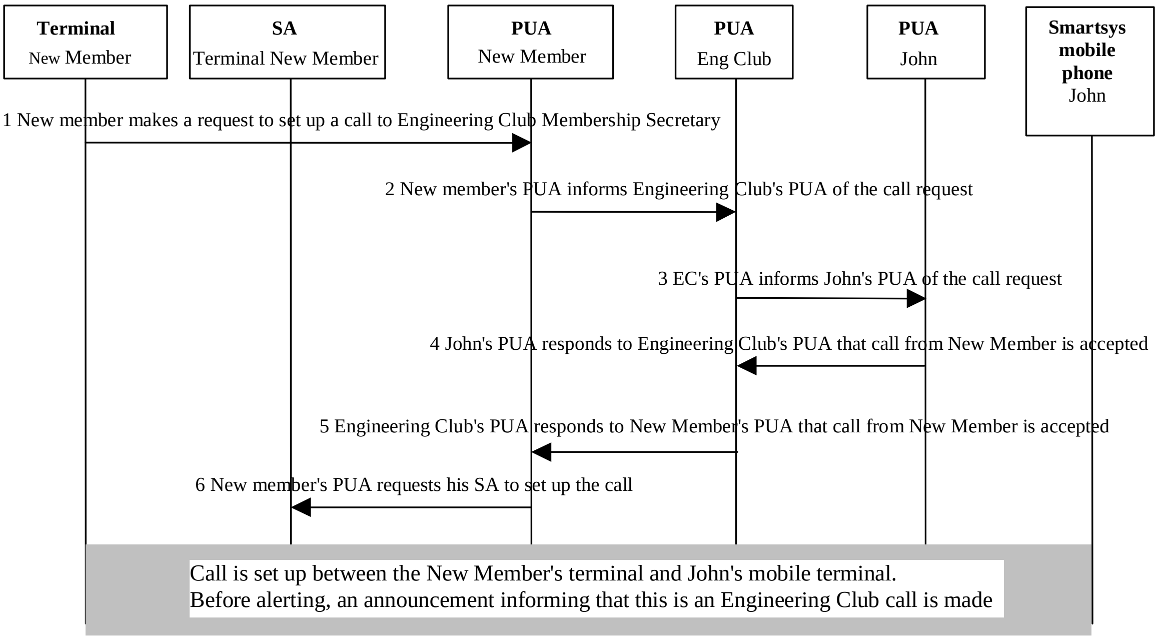

Terminal
New Member
SA
Terminal New Member
PUA
New Member
PUA
Eng Club
PUA
John
Smartsys mobile phone
John
1 New member makes a request to set up a call to Engineering Club Membership Secretary
2 New member's PUA informs Engineering Club's PUA of the call request
3 EC's PUA informs John's PUA of the call request
4 John's PUA responds to Engineering Club's PUA that call from New Member is accepted
5 Engineering Club's PUA responds to New Member's PUA that call from New Member is accepted
6 New member's PUA requests his SA to set up the call
Call is set up between the New Member's terminal and John's mobile terminal.
Before alerting, an announcement informing that this is an Engineering Club call is made

Figure A.16: Multiple workplace - Step 2 - Inbound Engineering Club Communication

Flow	Parameters	Action
1 Call request from New Member sent to his PUA	Called Party Identity = Engineering Club UCI <numeric> Calling Party Identity = New Member UCI <label; numeric> Service Type = P-P real-time voice QoS = PSTN voice	Normal call from new member to the Engineering Club's Membership Secretary.
2 New Member's PUA informs the engineering club's PUA of a call from a 'new member'	Called Party Identity = Engineering Club UCI <numeric> Calling Party Identity = New Member UCI <label; numeric> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	Normal call from new member to the Engineering Club's Membership Secretary.

3 Engineering club's PUA informs John's PUA of a call from a 'new member'	Called Party Identity = Engineering Club UCI <numeric>
	Calling Party Identity = New Member UCI <label; numeric>
	Command = Call request Service Type = P-P real-time voice
	QoS = PSTN voice
		Call indication redirected from Eng Club PUA to John's PUA retaining same caller and called Party identities.

4 John's PUA accepts the call from the new member	Called Party Identity = Engineering Club UCI <numeric>
	Calling Party Identity = New Member UCI <label; numeric>
	Command = Accept call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for John's PUA
		John's PUA accepts the call and provides routing information to set up the call to John's terminal.

Flow	Parameters	Action

5 Engineering Club's PUA accepts the call from the new member	Called Party Identity = Engineering Club UCI <numeric>
	Calling Party Identity = New Member UCI <label; numeric>
	Command = Accept call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for John's PUA
		Engineering Society's PUA accepts the call and relays the routing information to set up the call to John's terminal.

6 The New Member's PUA instructs his SA to establish a call from his terminal to John's terminal	Called Party Identity = Engineering Club UCI <numeric>
	Calling Party Identity = New Member UCI <label; numeric>
	Command = Establish call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for John's PUA
		The network is supplied with sufficient information to set up the call between the New Member's Terminal and John's Terminal.

NOTE: The New Member's SA establishes a call between his terminal and John's mobile terminal. Before alerting, an announcement informing this is an Engineering Club call is made.		

The SmartSys PUA informs John's PUA that a mobile is now available and that SmartSys is happy for it to receive personal incoming calls (at zero cost). At the earliest opportunity John's personal PUA will ask him if he wishes to define additional contact rules relating to the mobile. In the meantime, as a default, it assumes that if the mobile is turned on then John is available for calls that are acceptable (as defined in his user profile).

The caller sees only the club UCI as the recipient because the clubs PUA is the recipient as far as the originator is concerned.

Step 1 - Issues

- John's PUA is able to retain the calling and called party identities when delivering the call to John's mobile even though the terminal has been provided by SmartSys.

- John's PUA knows the capabilities of the mobile terminal and has to play an announcement prior to completing the speech path to the calling party.

A.5.3.3 Step 3 - Outbound Engineering Club Communication

Back in the house John turns on his PC, opens his PUA Profile Management application and requests communications history details. The call requesting membership details is at the top of the list, being the latest communication. John clicks on this and then selects "return" and "voice call" and accepts the default role offered - "membership secretary, engineering club".

John's PUA knows that this call was forwarded from the engineering club PUA. The PUA would offer the "membership secretary, engineering club" role as the default option for returned communications originating from the engineering club PUA. The returned communications would be labelled as "membership secretary, engineering club" and not "John Smith" (his own name). Alternatively, John could have selected "John Smith" which would have passed on his personal UCI rather than the club one.

The call is established and John can now pass over the details on annual fees from his club database.

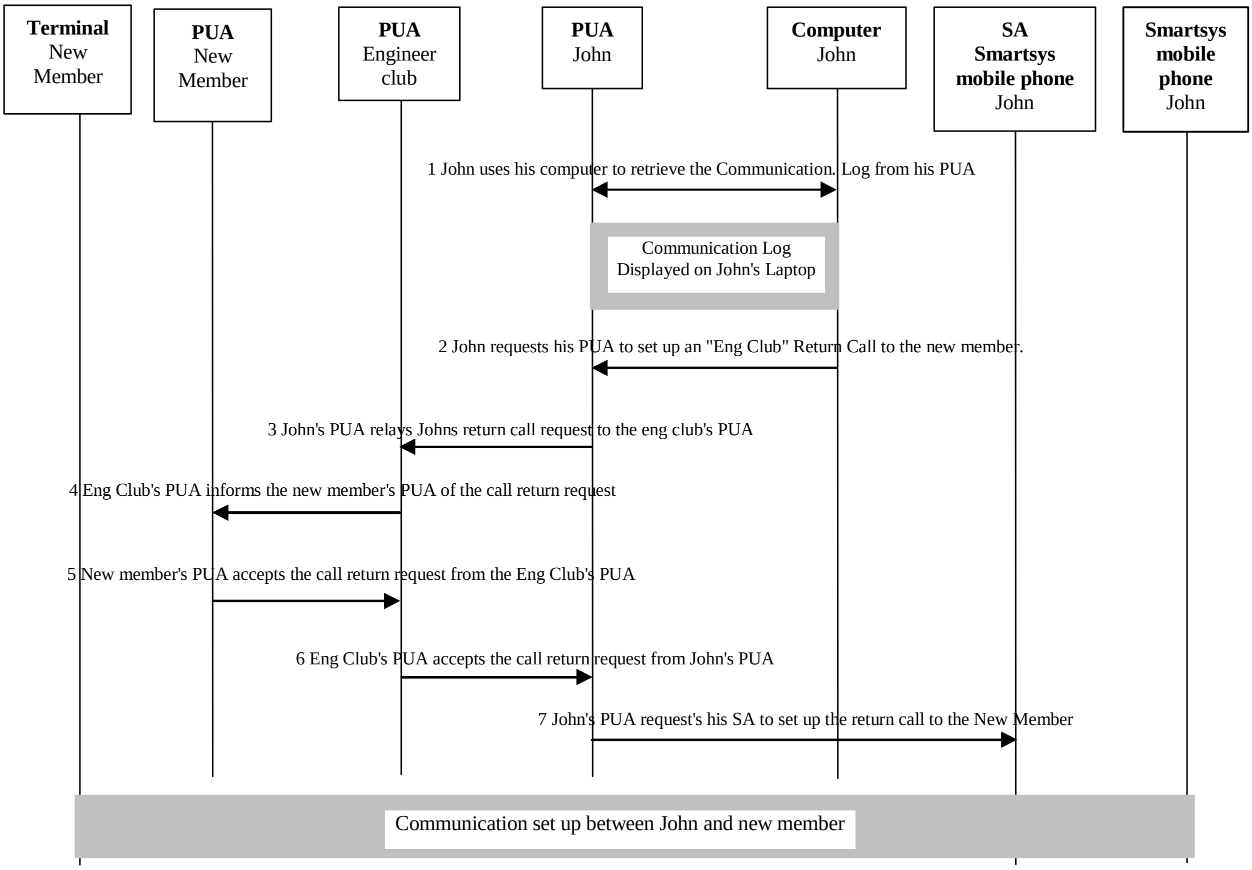

Terminal New Member
PUA New Member
PUA Engineer club
PUA John
Computer John
SA Smartsys mobile phone John
Smartsys mobile phone John
1 John uses his computer to retrieve the Communication. Log from his PUA
Communication Log Displayed on John's Laptop
2 John requests his PUA to set up an "Eng Club" Return Call to the new member.
3 John's PUA relays Johns return call request to the eng club's PUA
4 Eng Club's PUA informs the new member's PUA of the call return request
5 New member's PUA accepts the call return request from the Eng Club's PUA
6 Eng Club's PUA accepts the call return request from John's PUA
7 John's PUA request's his SA to set up the return call to the New Member
Communication set up between John and new member

Figure A.17: Multiple workplace - Step 3 - Outbound Engineering Club Communication

Flow	Parameters	Action

1 John uses his computer to retrieve the communication log request	User identity = John UCI
	Command = Search
	Source = John's PUA
	Search parameters = 'Last Call' and 'Engineering Club'
		John retrieves his communications log from his PUA that can be viewed according to criteria such as date ranges and contact names (UCI Labels). The retrieval queries are set for 'Last Call' and 'Engineering Club'. The PUA responds by returning the communications log details according to the query. The response is displayed on his laptop.

The retrieved communication log is displayed on John's computer.		
2 John uses his computer to set up an engineering club return call to the new member	Called Party Identity = New member UCI <label; number> Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	The PUA would offer the "membership secretary, engineering club" role as the default option for returned communications originating from the engineering club PUA.
3 John's PUA informs the Eng club's PUA of an engineering club return call request to the new member	Called Party Identity = New member UCI <label; number> Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	The returned communications would be labelled as "membership secretary, engineering club" and not "John Smith" (his own name).

Flow	Parameters	Action
4 The Engineering club's PUA informs the New Member's PUA of an engineering club return call request to the new member	Called Party Identity = New member UCI <label; number> Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	

5 The New Member's PUA responds to the Engineering club's PUA's that the engineering club return call is accepted	Called Party Identity = New member UCI <label; number>
	Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number>
	Command = Accept call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for New Member's Terminal	

6 The Engineering club's PUA responds to John's PUA's that the engineering club return call is accepted	Called Party Identity = New member UCI <label; number>
	Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number>
	Command = Accept call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Routing = PUA for Engineering Club
	Data = Routing information for New Member's Terminal	

7 John's PUA informs John's SA to set up the return call request	Called Party Identity = New member UCI <label; number>
	Calling Party Identity = Eng Club UCI < Label =Membership Secretary, Engineering Club, number>
	Command = Establish call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for New Member's Terminal
		The network is supplied with sufficient information to set up the call between John's Terminal and the New Member's Terminal.

NOTE: Call set-up would proceed as for a normal call. The call was set-up between John's default terminal and the prospective new member.		

Step 3 - Issues

- John's PUA is able to accept call set-up requests from John's PC.
- John's PUA is able to offer the calling party identity of the 'Membership Secretary, Engineering Club' instead of John's personal UCI details.

A.6 Corporate Scenario

A.6.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- how manager/secretary communications behaviour could be supported using UCIs (Most steps);
- how PUAs can instruct specialized applications (e.g. a manager/secretary communications controller) to perform tasks without involving human intervention (Step 3);
- how information on the UCI owner (e.g. information such as if they are staying in a hotel) can be used to significantly alter the normal communication behaviour (Step 5);
- how the PUA can use Presence information (e.g. no access to email service) and command external specialized services (e.g. an email to fax translation server) to determine when it will be necessary to take one form of communication and transform it into a different medium (e.g. forwarding selected emails to a hotel as faxes) (Step 6).

A.6.2 Scenario description

In a corporate or business environment, a corporate PUA would contain the PUAs that represent roles within the group. Such an arrangement would enable the benefits of a UCI and its supporting architecture to be available to organizations typically employing PABXs. Many functions of the PABX would be reproduced by the functionality and interactions of the corporate PUA. This scenario shows how the capability of a UCI based system could augment the organizational efficiency of a traditional manager/secretary relationship.

Table A.5: Corporate Scenario

Scenario Description	Technical Notes
BACKGROUND	
Steve is Managing Director of a large company importing fashion goods and is keen to keep very tight control on his communications so that he can work at maximum efficiency. He wants his secretary Sally to handle the majority of his communications while he is in the office, but he wants all email or phone calls from his wife, Christine, and his boss Albert to go directly to him. During the day Steve can get on with his work while Sally handles the day-to-day tasks arising from routine emails and phone calls.	Steve's PUA will, by default, offer Sally's communication addresses as the connection points for all his incoming communications. There needs to be the option of offering Sally or Steve's UCI identity to the sender. Sally's communication addresses will be obtained by interrogating her PUA on a call-by-call basis. As Christine and Albert both have UCIs, Steve's PUA can easily identify incoming communication requests from them and ensure that they are handled directly and not offered to Sally. If Christine called from a public telephone without registering her UCI she could still be connected to Steve by Sally in the traditional way.
STEP 1,2 Steve gets his wife's email reminding him to get home early and a call from Albert asking him to handle the monthly Management Meeting.	His PUA is set-up to receive communications from these two directly.
STEP 3 Towards the end of the day Sally has an incoming call from the organizer of the conference at which Steve will be speaking.	Sally gets the call as determined by Steve's PUA.
Sally realizes that Steve needs to speak to him and is able to click an icon on her PC which switches the call through to Steve.	A PC based secretarial communications application, supported by Sally's PUA and the office telephony SA, provides all the usual facilities required in this situation such as intercom control and call forwarding. Steve's PUA directs the call to his mobile because he has already left the office.
STEP 4 Sally uses the Internet to book a hotel for Steve when he goes to participate at the Conference in Vienna. Steve leaves for the meeting and checks in to the hotel.	Steve's PUA automatically updates his user profile with implications of hotel booking. (i.e. remotely located for three days).
STEP 5 During the next day Steve switches off his mobile during the conference. A call from his wife is directed to voice mail and an SMS message is automatically sent to the mobile to inform him.	Steve's PUA knows that the mobile is switched off (from a Presence Service) and hence uses the combination of voice mail and SMS.
STEP 6 Sally is still getting routine emails and phonecalls. She feels that the email from the Finance Director is important and forwards it to Steve. It is automatically converted to a fax and sent to Steve's hotel as well.	Steve's PUA knows, from his location, that he may not have email access but the hotel booking details list the hotel fax number.

A.6.3 Discussion

A.6.3.1 Step 1 - Incoming email from Steve's wife

Steve is Managing Director of a large company importing fashion goods and is keen to keep very tight control on his communications so that he can work at maximum efficiency. He wants his secretary Sally to handle the majority of his communications while he is in the office, but he wants all email or phone calls from his wife, Christine, and his boss Albert to go directly to him. During the day Steve can get on with his work while Sally handles the day-to-day tasks arising from routine emails and phone calls.

Steve gets his wife's email reminding him to get home early.

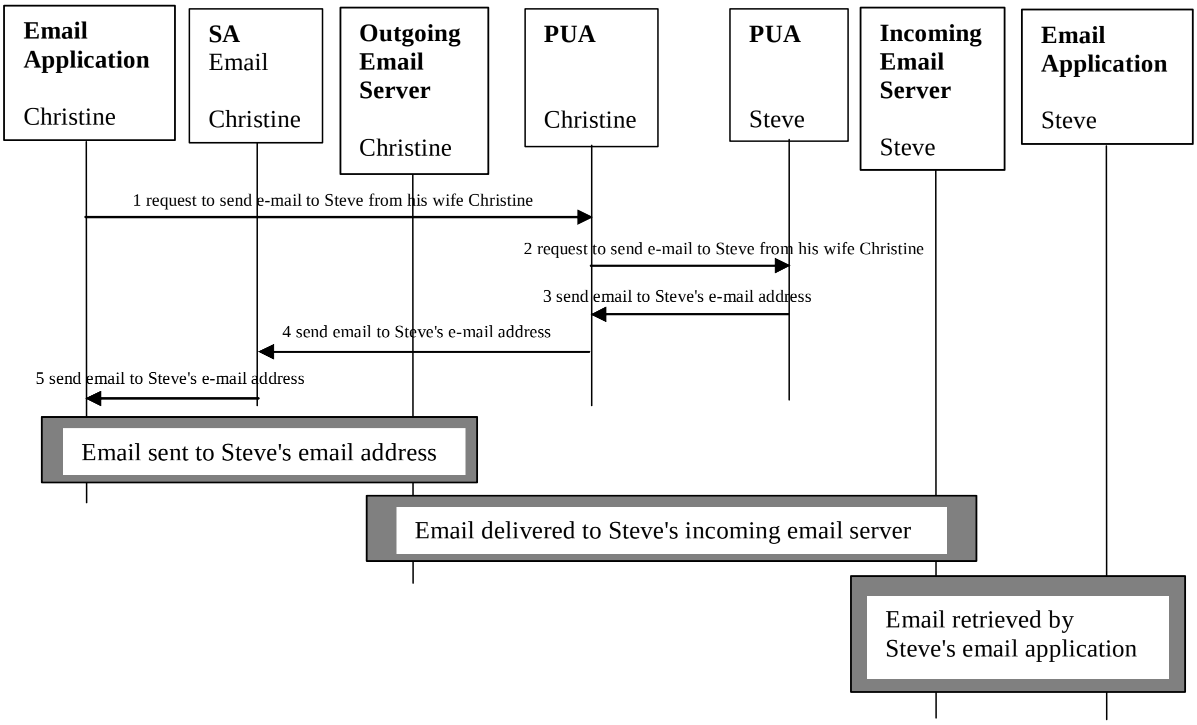

Email Application
Christine
SA Email
Christine
Outgoing Email Server
Christine
PUA
Christine
PUA
Steve
Incoming Email Server
Steve
Email Application
Steve
1 request to send e-mail to Steve from his wife Christine
2 request to send e-mail to Steve from his wife Christine
3 send email to Steve's e-mail address
4 send email to Steve's e-mail address
5 send email to Steve's e-mail address
Email sent to Steve's email address
Email delivered to Steve's incoming email server
Email retrieved by Steve's email application

Figure A.18: Corporate - Step 1 - Incoming email from Steve's wife

Flow	Parameters	Action
1 Christine sends a request to her PUA to send an email to Steve	Called Party Identity = Steve UCI <numeric> Service Type = Email	Christine sends an email to Steve's UCI.
2 Chrisitine's PUA informs Steve's PUA of an email request	Called Party Identity = Steve's UCI <numeric> Calling Party Identity = Christine UCI <label; numeric> Command = Email request Service Type = Email	Christine's PUA negotiates with Steve's PUA for the email
3 Steve's PUA responds to Christine's PUA that the email should be sent to Steve's email address	Called Party Identity = Steve's UCI <label, numeric> Calling Party Identity = Christine UCI <label; numeric> Command = Accept email Service Type = Email Data = Routing information for Steve's email account	Steve's PUA knows which email accounts he is likely to be reading and sends details of one of them in return.
4 Christine's PUA requests her email service to send an email to Steve's email account	Calling Party Identity = Christine UCI <label; numeric> Called Party Identity = Steve's UCI <label, numeric> Command = Send email Service Type = Email Data = Routing information for Steve's email account	The email service is supplied sufficient information to direct the email to Steve's chosen account.

5 Christine's email service provides the destination information and initiates the send action	Called Party Identity = Steve's email account
	Command = Send
	Message = Message Christine entered
	Attachment = Christine's UCI
		Christine's email service supplies the information to populate the "To" field of the email and also Christine's UCI as an email attachment

NOTE 1: An email is sent from Christine's Email application to her Outgoing Email Server. NOTE 2: Christine's outgoing email server delivers the email to Steve's incoming email server. NOTE 3: Steve retrieves the email when he next reads email from the selected account.		

Step 1 - Issues

- Steve's email details are provided to Christine's email application. In the interests of not revealing service specific identifiers, it may be necessary to use a temporary email address or a restricted functionality email account to receive emails sent using UCIs.
- The mechanism has to be available for incoming email server to arrange for SMS messages to be delivered on receipt of incoming emails.

A.6.3.2 Step 2 - Incoming voice call from Albert

Steve gets a call from Albert asking him to handle the monthly Management Meeting.

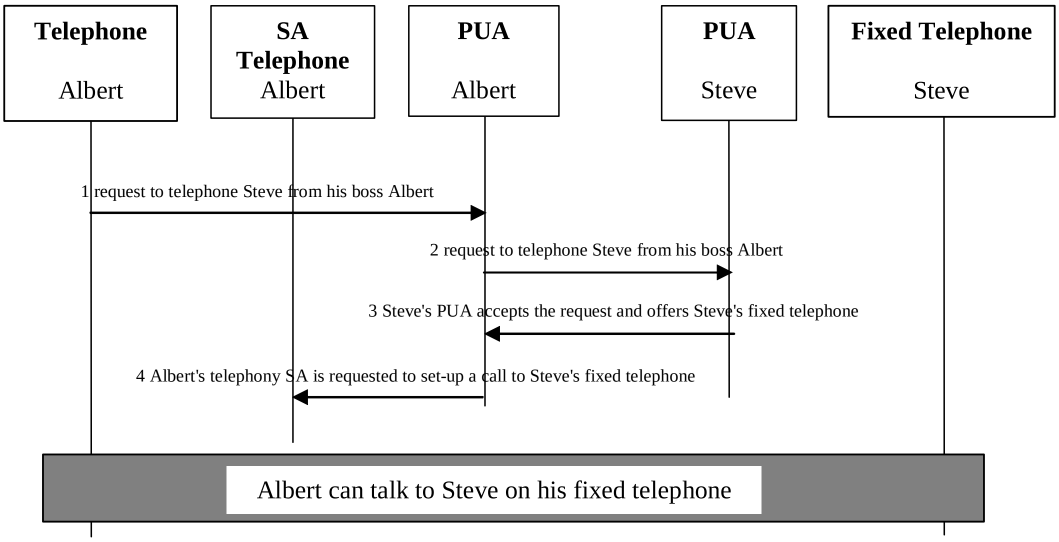

Telephone
Albert
SA Telephone
Albert
PUA
Albert
PUA
Steve
Fixed Telephone
Steve
1 request to telephone Steve from his boss Albert
2 request to telephone Steve from his boss Albert
3 Steve's PUA accepts the request and offers Steve's fixed telephone
4 Albert's telephony SA is requested to set-up a call to Steve's fixed telephone
Albert can talk to Steve on his fixed telephone

Figure A.19: Corporate - Step 2 - Incoming voice call from Albert

Flow	Parameters	Action
1 Incoming call from Albert	Called Party identity = Steve UCI <number> Calling Party identity = Albert UCI <label, number> Service Type = P-P real-time voice QoS = PSTN voice	Steve's PUA applies profile to incoming voice call
2 voice call routed to Steve's fixed phone	Called Party identity = Steve UCI <number> Calling Party identity = Albert UCI <label, number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	PUA rules determine Steve will accept voice calls from Albert, so this is routed to Steve's fixed phone.

3 Steve's PUA responds to Albert's PUA that the call from Albert is accepted	Called Party Identity = Steve UCI <label, numeric>
	Calling Party Identity = Albert UCI <label, numeric>
	Command = Accept call
	Service Type = P-P real-time voice
	QoS = PSTN Voice
	Data = Routing information for Steve's fixed telephone
		Steve's PUA knows he is available on his fixed phone and offers that to Albert.

4 Albert's PUA informs Albert's SA to set up the new call request	Calling Party Identity = Albert UCI <label, numeric>
	Called Party Identity = Steve UCI <label, numeric>
	Command = Establish call
	Service Type = P-P real-time voice
	QoS = PSTN Voice
	Data = Routing information for Steve's fixed telephone
		The network is supplied sufficient information to set up the call between Albert's telephone and Steve's fixed telephone.

NOTE: A call between Albert and Steve on his fixed phone is established.		

A.6.3.3 Step 3 - Incoming voice call from conference organizer

Towards the end of the day Sally has an incoming call from the organizer of the conference at which Steve will be speaking. Sally realizes that Steve needs to speak to him and is able to click an icon on her PC which switches the call through to Steve. A PC based secretarial communications application provides all the usual facilities required in this situation such as intercom control and call forwarding.

Steve's PUA directs the call to his mobile because he has already left the office.

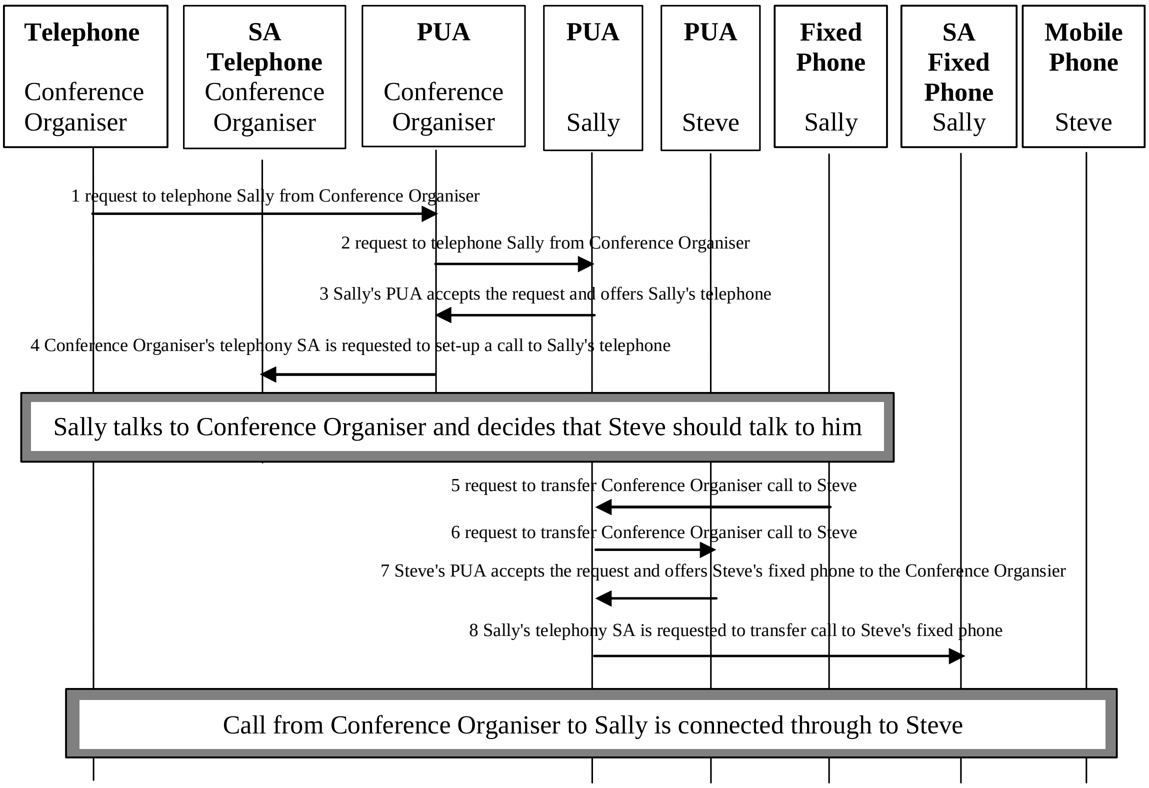

Telephone
Conference Organiser
SA Telephone
Conference Organiser
PUA
Conference Organiser
PUA
Sally
PUA
Steve
Fixed Phone
Sally
SA Fixed Phone
Sally
Mobile Phone
Steve
1 request to telephone Sally from Conference Organiser
2 request to telephone Sally from Conference Organiser
3 Sally's PUA accepts the request and offers Sally's telephone
4 Conference Organiser's telephony SA is requested to set-up a call to Sally's telephone
Sally talks to Conference Organiser and decides that Steve should talk to him
5 request to transfer Conference Organiser call to Steve
6 request to transfer Conference Organiser call to Steve
7 Steve's PUA accepts the request and offers Steve's fixed phone to the Conference Organsier
8 Sally's telephony SA is requested to transfer call to Steve's fixed phone
Call from Conference Organiser to Sally is connected through to Steve

Figure A.20: Corporate - Step 3 - Incoming voice call from conference organizer

Flow	Parameters	Action
1 Conference Organizer sends a request to his PUA to set-up a call to Sally	Called Party identity = Sally UCI <number> Service Type = P-P real-time voice QoS = PSTN voice	Conference Organizer makes a call to Sally's UCI.
2 Conference Organizer's PUA informs Sally's PUA of a new call request	Called Party identity = Sally UCI <number> Calling Party identity = Conf org UCI <label; number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	Conference Organizer's PUA offers call to Sally's PUA.

3 Sally's PUA responds to the Conference Organizer's PUA that the call from Sally is accepted	Called Party Identity = Sally UCI <number>
	Calling Party Identity = Conf org UCI <label; number =withheld>
	Command = Accept Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Sally's Work Phone
		Sally's PUA confirms acceptance of the call request to Conference Organizer's PUA.

Flow	Parameters	Action

4 Conference Organizer's PUA instructs his SA to set up a call to Sally's Work Phone	Called Party Identity = Sally UCI <number>
	Calling Party Identity = Conf Organizer UCI <label; number>
	Command = Establish Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Sally's Work Phone
		On receipt of the confirmation from Sally's PUA, the Conference Organizer's PUA progresses with the call request to Sally by supplying the network with sufficient information to set up the call to Sally's Work Phone.

A call between the Conference Organizer and Sally is established. The conversation reveals that Steve should talk to the Conference Organizer. NOTE: Sally may speak to Steve before forwarding the call to him. In this case, a further standard interchange between PUAs and SAs (as in steps 1-4 above) will take place to establish a call between Sally and Steve. When this call has terminated the procedure will continue as in the steps below.		

5 Sally sends a request to her PUA to transfer a call to Steve	Called Party identity = Steve UCI <number>
	Command = Call transfer
	Service Type = P-P real-time voice
	QoS = PSTN voice
		Sally contacts her PUA to arrange a transfer.

6 Sally's PUA informs Steve's PUA of a call transfer request	Called Party identity = Steve UCI <number> Calling Party identity = Conf org UCI <label; number> Command = Call transfer Service Type = P-P real-time voice QoS = PSTN voice	Sally's PUA offers call transfer to Steve's PUA.

7 Steve's PUA responds to Sally's PUA that the call transfer from the Conference Organizer is accepted	Called Party Identity = Steve UCI <number>
	Calling Party Identity = Conf org UCI <label; number>
	Command = Accept Call transfer
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Steve's Mobile Phone
		Steve's PUA confirms acceptance of the call transfer request to Steve's PUA proposing Steve's mobile phone.

8 Sally's PUA instructs her SA to set up the call transfer to Steve's mobile phone	Called Party Identity = Steve UCI <number>
	Calling Party Identity = Conf Organizer UCI <label; number>
	Command = Establish Transferred Call
	Service Type = P-P real-time voice
	QoS = PSTN voice
	Data = Routing information for Steve's Mobile Phone
		On receipt of the confirmation from Steve's PUA, Sally's PUA progresses with the call transfer request to Steve by supplying the network with sufficient information to set up the call to Steve's Mobile Phone.

NOTE: The call from the Conference Organizer to Sally is now extended to Steve's mobile telephone and Sally is disconnected.		

Step 3 - Issues

- Mechanism needed to provide Secretary/Manager intercom facility.

- Issues about the ownership of certificates and rights of use (e.g. Sally using Steve's certificate).

A.6.3.4 Step 4 - Automatic update of user profile

Sally uses the Internet to book a hotel for Steve when he goes to participate at the Conference in Vienna. Steve leaves for the meeting and checks in to the hotel.

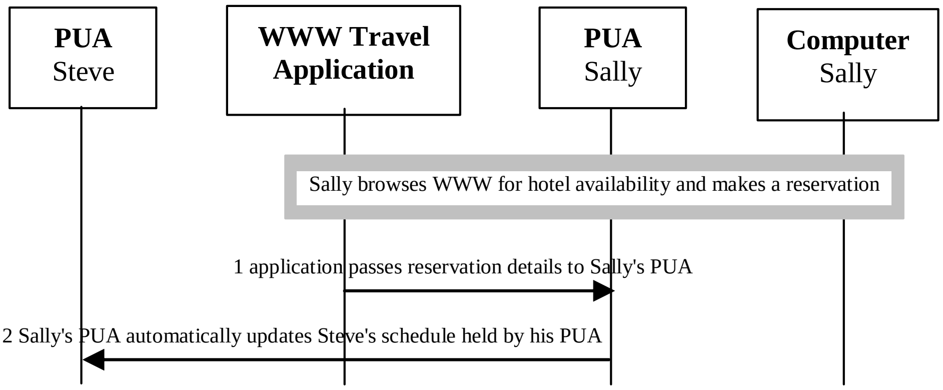

PUA
Steve
WWW Travel
Application
PUA
Sally
Computer
Sally
Sally browses WWW for hotel availability and makes a reservation
1 application passes reservation details to Sally's PUA
2 Sally's PUA automatically updates Steve's schedule held by his PUA

Figure A.21: Corporate - Step 4 - Automatic update of user profile

Flow	Parameters	Action
Sally browses the web and makes a hotel reservation for Steve using a site that sends back booking confirmations.		
1 www application passes reservation confirmation to Sally's PUA	Called Party identity = Sally UCI <number> Calling Party identity = www application UCI <label; number> Command = schedule information Service Type = data transfer Data = reservation information	Sally browses WWW for hotel availability and room rates. Then she selects and makes a reservation for Steve.
2 Sally's PUA updates Steve's schedule held by his PUA	Called Party identity = Steve UCI <number> Calling Party identity = Sally UCI <label; number> Command = schedule information Service Type = data transfer Data = reservation information	Sally's PUA automatically updates Steve's schedule to include his hotel reservation details (feedback to Steve should also be provided).

Step 4 - Issues

- Mechanism to support update of schedule information by a 3rd party may be standardized or proprietary.

A.6.3.5 Step 5 - Do NOT Disturb!

During the next day Steve switches off his mobile during the conference. A call from his wife, Christine, is directed to voice mail and an SMS message is automatically sent to the mobile to inform him.

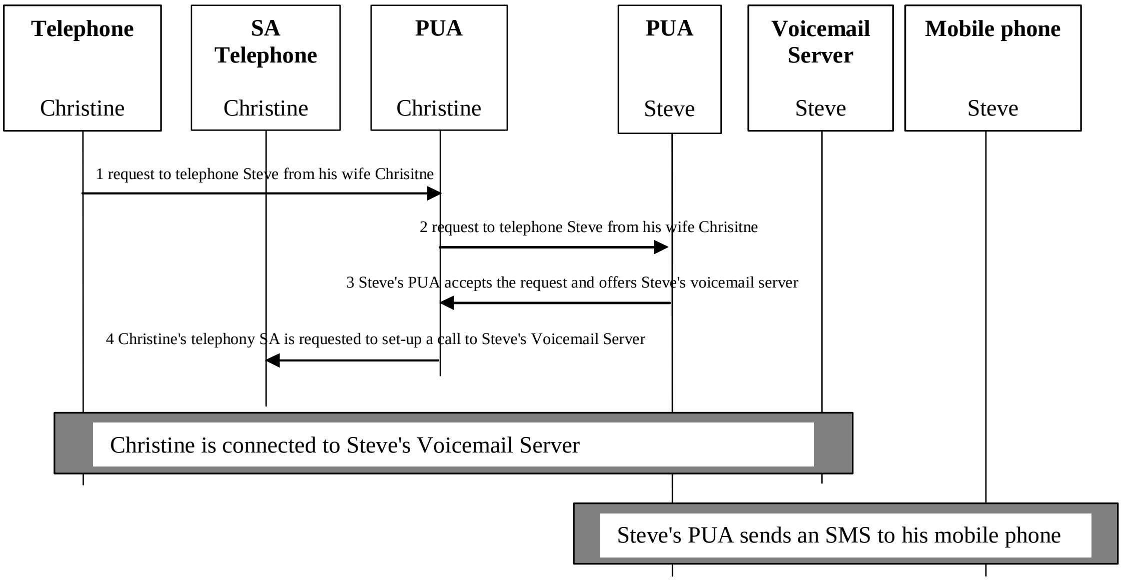

Telephone
Christine
SA Telephone
Christine
PUA
Christine
PUA
Steve
Voicemail Server
Steve
Mobile phone
Steve
1 request to telephone Steve from his wife Chrisitne
2 request to telephone Steve from his wife Chrisitne
3 Steve's PUA accepts the request and offers Steve's voicemail server
4 Christine's telephony SA is requested to set-up a call to Steve's Voicemail Server
Christine is connected to Steve's Voicemail Server
Steve's PUA sends an SMS to his mobile phone

Figure A.22: Corporate - Step 5 - Do NOT Disturb!

Flow	Parameters	Action
1 Christine sends a request to her PUA to set-up a voice call to Steve	Called Party identity = Steve UCI <number> Service Type = P-P real-time voice QoS = PSTN voice	Christine makes a call to Steve's UCI.
2 Christine's PUA informs Steve's PUA of a new call request	Called Party identity = Steve UCI <number> Calling Party identity = Christine UCI <label; number> Command = Call request Service Type = P-P real-time voice QoS = PSTN voice	Christine's PUA offers call to Steve's PUA.

3 Steve's PUA responds to the Christine's PUA that the call can be accepted as voicemail	Called Party Identity = Steve UCI <number>
	Calling Party Identity = Christine UCI <label; number>
	Command = Accept Call
	Service Type = P-P stored voice
	QoS = PSTN voice
	Data = Routing information for Steve's voicemail server
		Steve's PUA confirms acceptance of the call request to Christine's PUA with an indication of a stored voice service rather than a real-time voice service.

4 Christine's PUA instructs her SA to set up a call to Steve's voicemail	Called Party Identity = Steve UCI <number>
	Calling Party Identity = Christine UCI <label; number>
	Command = Establish Call
	Service Type = P-P stored voice
	QoS = PSTN voice
	Data = Routing information for Steve's voicemail server
		On receipt of the confirmation from Steve's PUA, Christine's PUA progresses with the call request to Steve by supplying the network with sufficient information to set up the call to Steve's voicemail server.

NOTE 1: Christine is connected to Steve's voicemail service and leaves a message. NOTE 2: Steve's PUA sends an SMS to his mobile telephone notifying him of a voice message from Christine.		

Step 5 - Issues

- Steve's PUA must know he is unavailable to receive voice calls.
- When Steve's PUA replies offering a stored voice service rather than a real-time voice service, the PUAs may wish to perform additional negotiation before Christine's PUA accepts an offer.

- Steve's PUA must receive sufficient details about the voice message to construct a satisfactory SMS which is sent to Steve's mobile phone.

A.6.3.6 Step 6 - Email redirected and delivered as FAX

Sally is still getting routine emails and phone calls. She feels that the email from the Finance Director is important and forwards it to Steve. It is automatically converted to a fax and delivered to Steve's hotel as well.

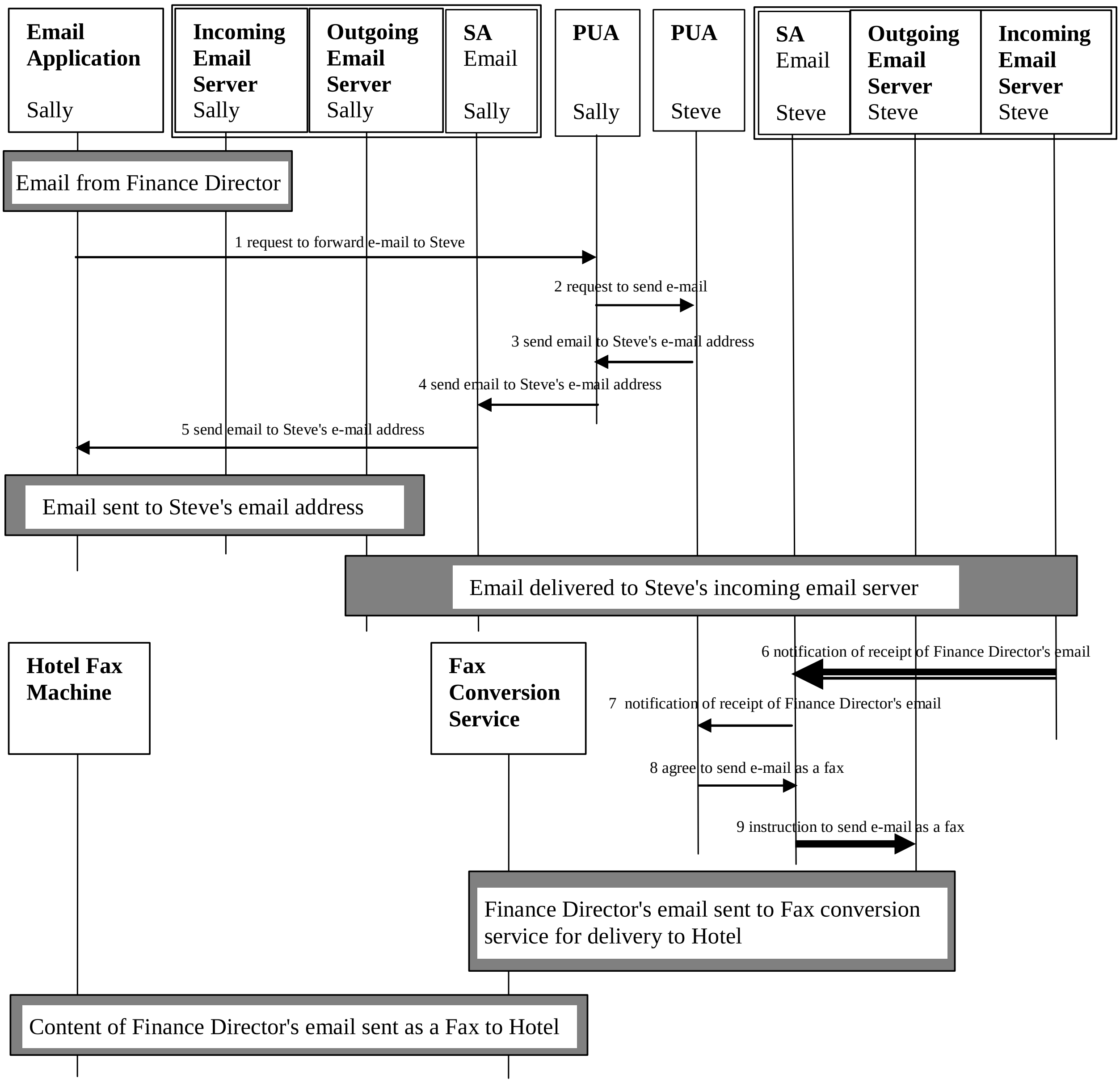

Email Application Sally
Incoming Email Server Sally
Outgoing Email Server Sally
SA Email Sally
PUA Sally
PUA Steve
SA Email Steve
Outgoing Email Server Steve
Incoming Email Server Steve
Email from Finance Director
1 request to forward e-mail to Steve
2 request to send e-mail
3 send email to Steve's e-mail address
4 send email to Steve's e-mail address
5 send email to Steve's e-mail address
Email sent to Steve's email address
Email delivered to Steve's incoming email server
Hotel Fax Machine
Fax Conversion Service
6 notification of receipt of Finance Director's email
7 notification of receipt of Finance Director's email
8 agree to send e-mail as a fax
9 instruction to send e-mail as a fax
Finance Director's email sent to Fax conversion service for delivery to Hotel
Content of Finance Director's email sent as a Fax to Hotel

Figure A.23: Corporate - Step 6 - Email redirected and delivered as FAX

Flow	Parameters	Action
Sally retrieves the Finance Director's email when she reads her email from the incoming mail server. She reads it and decides that it is important and needs to be forwarded to Steve.		
1 Sally sends a request to her PUA to forward the Finance Director's email to Steve	Called Party Identity = Steve UCI <numeric> Service Type = Email	Sally requests that the Finance Director's email is sent to Steve's UCI.
2 Sally's PUA informs Steve's PUA of an email request	Called Party Identity = Steve's UCI <numeric> Calling Party Identity =Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Command = Email request Service Type = Email	Sally's PUA asks to send an email to Steve's PUA.
3 Steve's PUA responds to Sally's PUA that the email should be sent to Steve's email address	Called Party Identity = Steve's UCI <label, numeric> Calling Party Identity = Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Command = Accept email Service Type = Email Data = Routing information for Steve's email account	Steve's PUA knows which email accounts he is likely to be reading and sends details of one of them in return.
4 Sally's PUA requests her email service to send an email to Steve's email account	Calling Party Identity = Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Called Party Identity = Steve's UCI <label, numeric> Command = Send email Service Type = Email Data = Routing information for Steve's email account	The email service is supplied sufficient information to direct the email to Steve's chosen account.

5 Sally's email service provides the destination information and initiates the send action	Called Party Identity = Steve's email account
	Command = Send
	Message = Message sent by Finance Director; Sally
	Attachment = Finance Director's UCI; Sally's UCI
		Sally's email service supplies the information to populate the "To" field of the email and also the Finance Director's and Sally's UCIs as email attachments.

An email is sent from Sally's Email application to her Outgoing Email Server.		
Sally's outgoing email server delivers the email to Steve's incoming email server		

6 Steve's incoming email server notifies his email SA of the receipt of the Finance Directors email	User identity = Steve UCI
	Command = Email notify receipt
	Source = Finance Director UCI; Sally UCI
	Item = Finance Directors email
		The email receipt notification contains the UCIs of the Finance Director and Sally.

7 Steve's email SA informs Steve's PUA of an email request	Called Party Identity = Steve UCI <numeric> Calling Party Identity =Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Command = Email notify receipt	Steve's SA asks Steve's PUA to send an email to Steve.
8 Steve's PUA requests his email service SA to send an email to the Fax Conversion Service for delivery as a Fax to the hotel	Calling Party Identity = Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Called Party Identity = Hotel Fax Number Command = Send email Service Type = Email Data = Routing information for the Fax conversion service	The email service is supplied sufficient information to direct the email to the Fax conversion service with details of the Hotel Fax number and The Finance Director's and Sally's UCIs.

Flow	Parameters	Action
9 the email service SA instructs the outgoing email server to send the Finance Director's email to the Fax Conversion Service	Calling Party Identity = Finance Director UCI <label; numeric>; Sally UCI <label; numeric> Called Party Identity = Hotel Fax Number Command = Send email Service Type = Email QoS = Data = Routing information for the Fax conversion service	The email service ensures that the outgoing mail server is given the information necessary to fully inform the Fax Conversion Service.
NOTE 1: The original Finance Director email plus the Hotel Fax number and the Finance Director's and Sally's UCIs are sent by email to the Fax conversion service. NOTE 2: Fax conversion service faxes the content of the email to the Hotel - with both the Finance Director's and Sally's UCI information in the sender fields of the fax.		

Step 6 - Issues

- Steve's PUA must already know that, while away, Steve needs his emails from Sally forwarded to him at his hotel fax.
- Steve's Email SA must be programmed to ensure that an email receipt notification message is sent to his PUA each time an email arrives.
- Steve's PUA must know the location of a Fax Conversion Service.
- Where forwarding occurs, it must be possible to convey the UCI of the communication originator and the UCI of the forwarder.

A.7 PUA acting as a personal assistant scenario

A.7.1 Key UCI capabilities illustrated by this scenario

As well as basic UCI-based communication, as described in clauses 9 and 10 of the present document, this scenario illustrates the following UCI capabilities:

- the ability of PUAs to exchange selected items from the user schedule information that they hold. This can be used to determine when real-time communication between two or more people can occur (Step 1);
- the ability of PUAs to alert their users of upcoming scheduled communications (Step 2);
- the use of the language information contained in UCI additional information fields to determine when specialized services such as translation services may be required (Step 3);
- the ability of a PUA to locate and utilize external servers to perform specialized tasks associated with a communication (e.g. the use of a translation server to transcribe text to a different language) (Step 3).

A.7.2 Scenario description

In addition to the functionality associated with the corporate PUA, specialized applications could enable the enhancement of current office management applications and supplementary services. This scenario gives an example of one such application.

In this scenario, the main character Pedro works in an advertising company with branches all over the country.

Table A.6: Business Application Scenario

Scenario Description	Technical Notes
STEP 1 Yesterday he received a phone call from a Turkish businessman asking for a proposal. His first task of the day is to discuss this proposed advertising campaign with colleagues. He brings up the Conference Management Application on his PC and indicates that the conference is "urgent". He selects from his address book several colleagues, some at remote locations, and against each name he indicates whether their presence is essential or not, and whether a deputy is acceptable.	The conference call setup is done using a specialized application that has been designed to communicate with the user's PUA. Pedro's PUA sends out "urgent conference call" communication requests to the PUAs of a set of his colleagues (with a message indicating the desired start time of the conference).
Some time later his PC screen confirms that most of the colleagues he wished to speak to are available in their offices and are about to join him in the conference. In one case a colleague will be on his mobile and in another a deputy will be involved until the actual invitee terminates a phone call.	His colleagues PUAs will examine the availability and presence information they have about their owners and will, after checking with their owners, confirm or reject the request.
STEP 2 The telephone rings and an announcement tells Pedro that the conference is beginning immediately. This is good news; on some other occasions the system has suggested booking a future timeslot to accommodate all required participants.	Pedro's PUA will alert Pedro and the invitees to the start of the conference call.
STEP 3 After the conference call, Pedro decides to send the proposal to his potential customer in Turkey. Pedro. He selects the customer's name from the address book prior to sending the proposal in the form of an email.	The customer's UCI was automatically stored in the communication history in Pedro's PUA when the customer called earlier.
However his PC immediately flags up the fact that his contact only reads fluently in French and Turkish (despite speaking Spanish well and reading it a little) and so Pedro decides to get the proposal translated into French before being sent the contact. He opts for an automated translation system selected by his PUA.	Pedro's PUA has examined the "preferred reading language" additional information field of his customer's UCI and noticed that Pedro's own language (Spanish) is not included.

A.7.3 Discussion

A.7.3.1 Step 1 - Scheduling a multiparty conference

Yesterday he received a phone call from a Turkish businessman asking for a proposal. His first task of the day is to discuss this proposed advertising campaign with colleagues. He brings up the Conference Management Application on his PC and indicates that the conference is "very high priority". He selects from his address book several colleagues, some at remote locations, and against each name he indicates whether their presence is essential or not, and whether a deputy is acceptable.

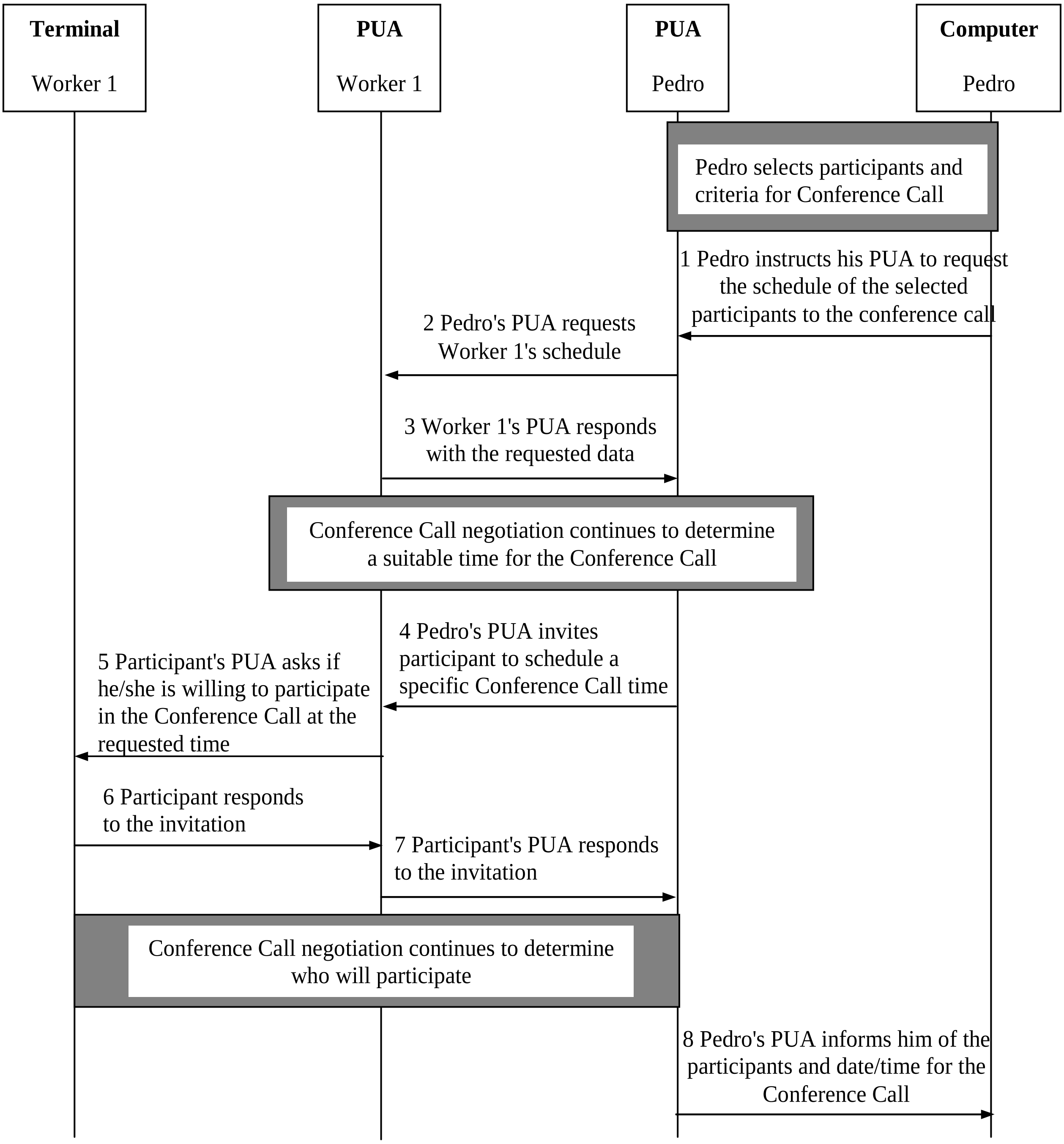

Terminal
Worker 1
PUA
Worker 1
PUA
Pedro
Computer
Pedro
Pedro selects participants and criteria for Conference Call
1 Pedro instructs his PUA to request the schedule of the selected participants to the conference call
2 Pedro's PUA requests Worker 1's schedule
3 Worker 1's PUA responds with the requested data
Conference Call negotiation continues to determine a suitable time for the Conference Call
4 Pedro's PUA invites participant to schedule a specific Conference Call time
5 Participant's PUA asks if he/she is willing to participate in the Conference Call at the requested time
6 Participant responds to the invitation
7 Participant's PUA responds to the invitation
Conference Call negotiation continues to determine who will participate
8 Pedro's PUA informs him of the participants and date/time for the Conference Call

Figure A.24: Personal assistant - Step 1 - Scheduling a multiparty conference

Flow	Parameters	Action

1 Selection of participants for conference call	User identity = Pedro UCI Private Identity
	Command = Propose Conference Call
	Source = Pedro's Conference Management application
	Item = List of participants (deputy acceptability criteria stated for each participant), preferred dates/times
		Pedro selects candidates for conference call and instructs his PUA to negotiate representation (including a deputy option) and start time.

2 Pedro's PUA invites Worker 1 to a potential conference call (time/date not yet finalized)	Called Party Identity = Worker 1 UCI Calling Party Identity = Pedro UCI Data = Conference Call proposal (set of dates/times, priority = "urgent")	The conference call setup is done using a specialized application that has been designed to communicate with PUAs. Pedro's PUA sends out a "urgent conference call" communication requests to the PUAs of a set of his colleagues (with a message indicating a range of desired dates and start times for the conference).
3 Worker 1's PUA responds to Pedro's invitation	Called Party Identity = Pedro UCI Calling Party Identity = Worker 1 UCI Data = Conference Call response (set of dates/times)	Participant or deputy and his availability (indicating acceptable dates/ times) identified to Pedro's PUA.
Processes 2 and 3 continue until all potential participants PUAs' have been contacted. Pedro's PUA can then finalize a date/time for the Conference.		
4 Pedro's PUA invites Worker 1 to a conference call at a finalized date and time	Called Party Identity = Worker 1 UCI Calling Party Identity = Pedro UCI Data = Conference Call proposal (date/time, priority = "urgent")	The invitation contains the date/time that was determined in the previous phase of negotiation.
5 Worker 1's PUA seeks Worker 1's agreement to participate in the conference call	Called Party Identity = Worker 1 terminal identity Calling Party Identity = Pedro UCI Data = Conference Call proposal (date/time, priority = "urgent", list of conflicts)	The proposed Conference Call details are forwarded to Worker 1. Any potential conflicts identified by Worker 1's PUA are also indicated.
6 Worker 1 responds with a "Yes" or "No"	Called Party Identity = Pedro UCI Calling Party Identity = Worker UCI Private Identity Data = Conference Call response (Yes/No)	Worker 1's indicates agreement or rejection of the invitation.
7 Worker 1's PUA forwards the response to Pedro's PUA	Called Party Identity = Pedro UCI Calling Party Identity = Worker 1 UCI Data = Conference Call response (Yes/No)	Worker 1's PUA forwards Worker 1's response to Pedro's PUA.
Processes 4, 5, 6 and 7 continue for all of the potential participants		
8 Pedro's PUA informs Pedro of the participants and the final date/time	Called Party Identity = Pedro terminal identity Calling Party Identity = Pedro PUA Identity Data = Conference Call response (date/time, list of participants)	Pedro's PUA summarized the responses from the PUA's of the invited participants and communicates this to Pedro.

Step 1 - Issues

- Inter-PUA communication needs to be supported.
- Release of schedule-like information requires security clearance.

A.7.3.2 Step 2 - Conference call in action

The telephone rings and an announcement tells Pedro that the conference is beginning immediately. This is good news; on some other occasions the system has suggested booking a future timeslot to accommodate all required participants.

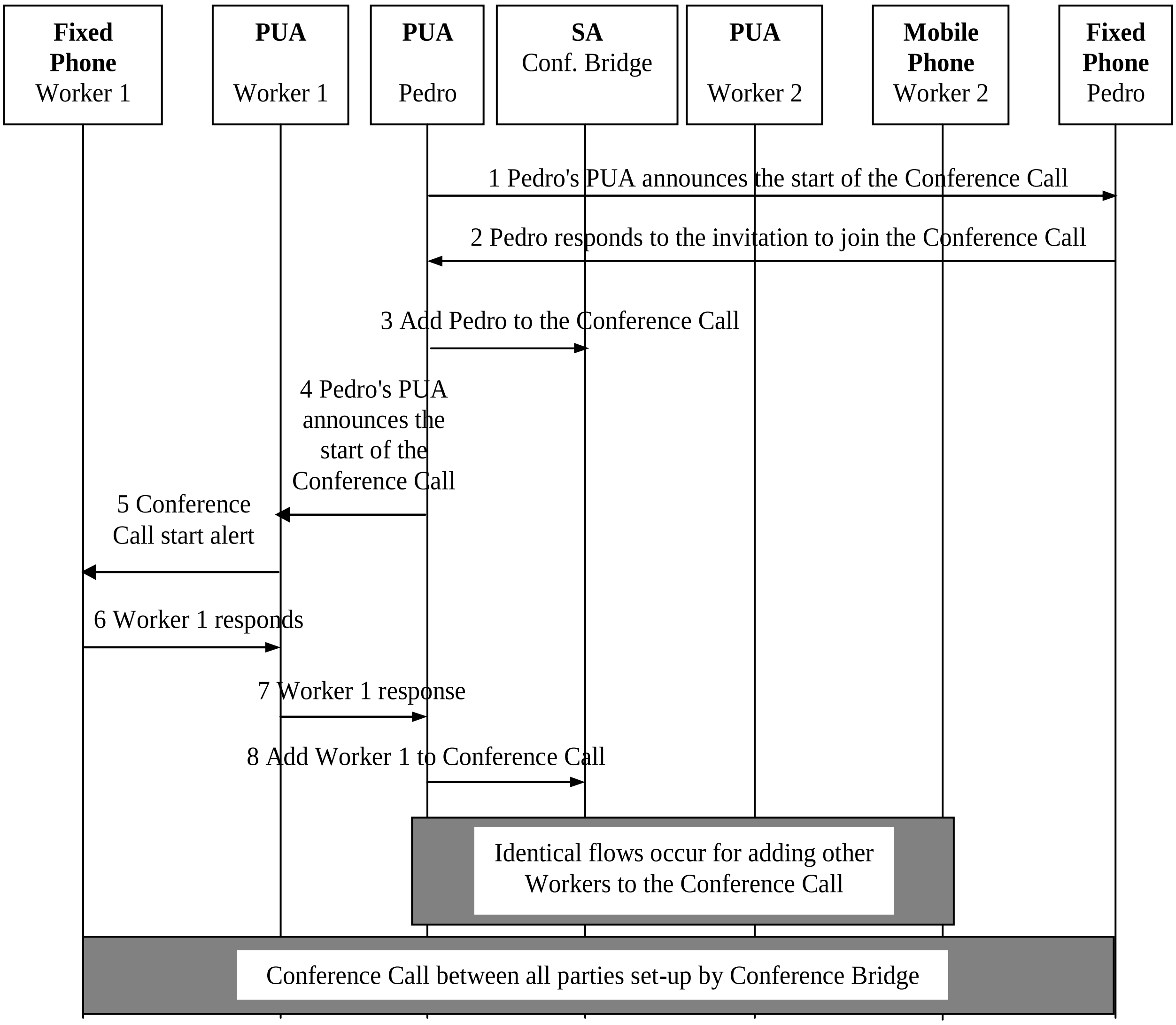

Fixed Phone Worker 1
PUA Worker 1
PUA Pedro
SA Conf. Bridge
PUA Worker 2
Mobile Phone Worker 2
Fixed Phone Pedro
1 Pedro's PUA announces the start of the Conference Call
2 Pedro responds to the invitation to join the Conference Call
3 Add Pedro to the Conference Call
4 Pedro's PUA announces the start of the Conference Call
5 Conference Call start alert
6 Worker 1 responds
7 Worker 1 response
8 Add Worker 1 to Conference Call
Identical flows occur for adding other Workers to the Conference Call
Conference Call between all parties set-up by Conference Bridge

Figure A.25: Personal assistant - Step 2 - Conference call in action

Flow	Parameters	Action
1 Pedro's PUA calls Pedro and announces start of conference call	Called Party Identity = Pedro terminal identity Calling Party Identity = Pedro PUA Identity Service Type = conference voice call request to join QoS = PSTN voice	Conference call is about to start and the conference chairman (Pedro) is invited to start the Conference Call.
2 Pedro responds to the invitation to join the Conference Call	Called Party Identity = Pedro UCI Calling Party Identity = Pedro UCI Private Identity Serviced Type = conference voice join acceptance Data = Pedro's voice contact address	Pedro replies to the communication which contacted his PUA.
3 Pedro added to the call	Called Party Identity = SA Identity for Conference Bridge Calling Party Identity = Pedro UCI Serviced Type = conference voice join acceptance Data = Pedro's voice contact address	Pedro's PUA passes Pedro's contact details to the Conference Bridge SA.
4 Pedro's PUA calls Worker 1 and announces start of conference call	Called Party Identity = Worker 1 UCI Calling Party Identity = Pedro UCI Service Type = conference voice call request to join QoS = PSTN voice	Conference call is about to start and the participant (Worker 1) is invited to join the Conference Call.
5 Worker 1's PUA forwards the invitation to join the Conference Call	Called Party Identity = Worker 1 terminal identity Calling Party Identity = Pedro UCI Serviced Type = conference voice call request to join QoS = PSTN voice	Worker 1 is told of the invitation to the Conference Call.
6 Worker 1 accepts the invitation to join Pedro's conference call	Called Party Identity = Pedro UCI Calling Party Identity = Worker 1 UCI Private Identity Service Type = conference voice join acceptance Data = Worker 1's voice contact address	Worker 1's PUA receives Worker once invitation acceptance.
7 Worker 1's PUA forwards the request to join conference call	Called Party Identity = Pedro UCI Calling Party Identity = Worker 1 UCI Service Type = conference voice join acceptance Data = Worker 1's voice contact address	Worker 1's PUA communicates acceptance to join the conference call.
8 Worker 1 added to the call	Called Party Identity = SA for Conference Bridge Calling Party Identity = Worker 1 UCI Serviced Type = conference voice join acceptance Data = Worker 1's voice contact address	Worker 1's PUA passes Worker 1's contact details to the Conference Bridge SA for connection. Worker 1's SA may be involved in the establishment of the media path.
NOTE 1: Flows such as 4, 5, 6, 7 and 8 are repeated for Worker 2 and all of the other active participants in the Conference Call. NOTE 2: The Conference Bridge uses the contact details passed to it by Pedro's PUA to set-up the Conference Call.		

Step 2 - Issues

- PUA initiation of conference call join.
- Multiparty conference call credentials need establishing.

A.7.3.3 Step 3 - email of proposal

After the conference call, Pedro decides to send the proposal to his potential customer in Turkey. Pedro. He selects the customer's name from the communication history prior to sending the proposal in the form of an email.

Pedro decides to get the proposal translated into French before transmission.

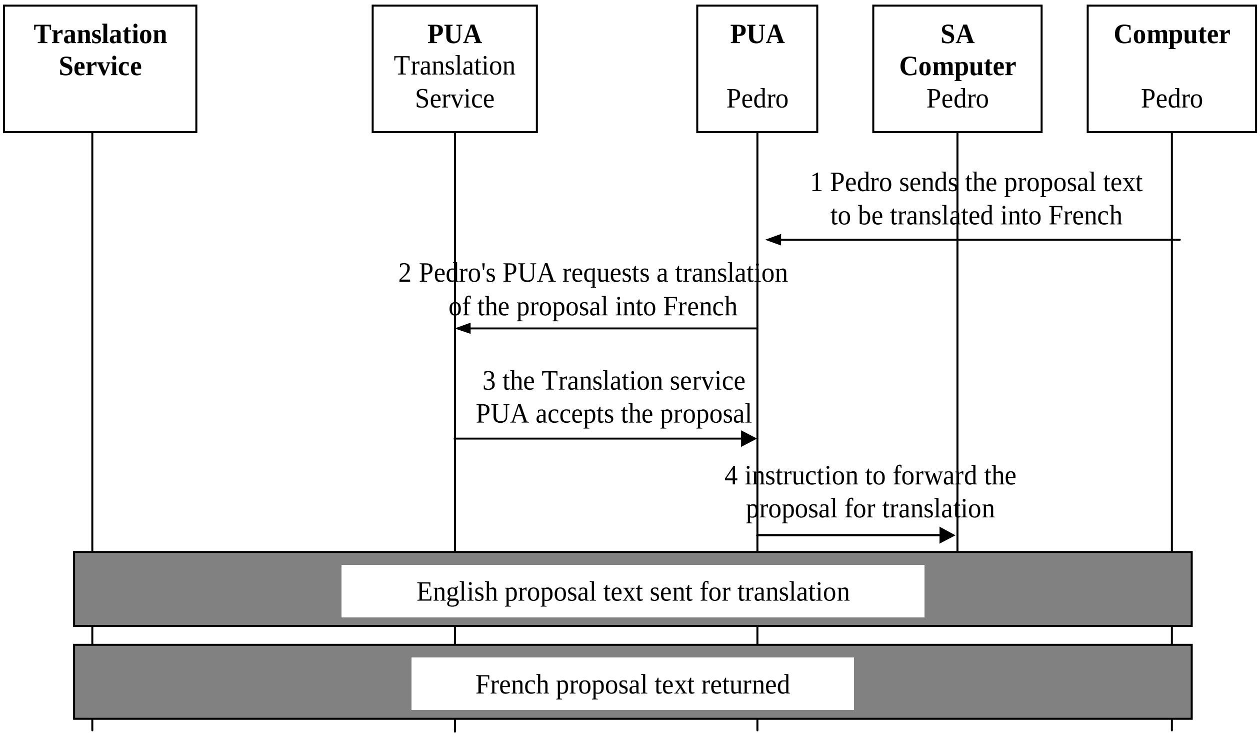

Translation Service
PUA Translation Service
PUA Pedro
SA Computer Pedro
Computer Pedro
1 Pedro sends the proposal text to be translated into French
2 Pedro's PUA requests a translation of the proposal into French
3 the Translation service PUA accepts the proposal
4 instruction to forward the proposal for translation
English proposal text sent for translation
French proposal text returned

Figure A.26: Personal assistant - Step 3 - email of proposal

Flow	Parameters	Action
1 Pedro's drafts proposal and emails to customer using the customer's UCI	Called Party Identity = Customer UCI Calling Party Identity = Pedro UCI Private Identity Service Type = email QoS = default email	Proposal attached to covering email with tag to translate into French.
Pedro's PUA arranges for the translation of the email and attachment (possibly using an external translation service)		
2 Pedro's PUA sends the translated email to the customer's PUA.	Called Party Identity = Customer UCI Calling Party Identity = Pedro UCI Service Type = email QoS = default email	Pedro's PUA forwards the translated email to the customer's PUA.
3 The customer's PUA forwards the email, together to the customer's email-server	Called Party Identity = Customer Mail-Server SA Identity Calling Party Identity = Pedro UCI Service Type = email QoS = default email	The customer's PUA attaches Pedro's UCI identity credentials to the email and sends it to the customer's email server.

Step 3 - Issues

- Email filtered/translated by PUA needs to be supported.
- <<Preferred reading language>> optional attribute needs to be supported.
- The PUA automatically stores incoming caller's UCI in the PUA communication history logs.

Annex B (informative): User Requirements for communications systems using UCIs

B.1 Notes relating to the user requirements

B.1.1 Origin of the user requirements

The requirements in this annex are those originally defined in EG 201 940 [1], with minor updates and clarifications.

B.1.2 Assumptions concerning the Universal Communications Identifier

Throughout this clause an assumption has been made that whenever a Universal Communications Identifier (UCI) is referred to, it will be as defined in EG 201 940 [1]. If a UCI adopted in the future is different to the one defined by EG 201 940 [1] then this will have significant implications for the technical implementation of many of the user requirements listed in this clause.

B.1.3 System re-engineering

User requirements, by definition, are not constrained by the technical issues which have to addressed when it comes to implementation. However, when the present document discusses the translation of user requirements into system capabilities and then into technical requirements, the emphasis has always been on minimising the changes required to existing networks, services and systems.

B.1.4 Dependencies and conflicts

It should be noted that some of these user requirements may wholly or in part conflict with other requirements; some support others requirements and some are dependent on other requirements. Dependencies and possible conflicts are summarized for each requirement. In developing any solutions based upon these requirements a judgement will clearly have to be made as to which requirements cannot be fully met.

B.2 Generic requirements

This clause examines the generic user requirements of a modern, ideal communications system. These will be used in subsequent clauses to derive more specific user requirements related to Human Factors and the UCI which will then in turn define system capabilities (annex B).

UR 1.1 Unifying the control of communications

Users, currently, can be faced with many options when wishing to set-up, receive and manage their communications. Typically people may possess a fixed telephone, a mobile telephone, a PC with a home email address, another PC at work, an email address and a fax machine. Each terminal, application and service will have a different identifier, and method of setting up, receiving and managing communications. Each will also have different levels of control (e.g. a user can send an email labelled "urgent" but not make a telephone call similarly labelled) and different methods of storing communication history.

An effective and efficient multi-modal communications system would have a choice of terminals, a single universal identifier and a common method of setting up, receiving and managing communications.

User requirement No UR 1.1
Users require a unified method of, and support for, setting up, receiving and managing communications that is, as far as possible, independent of the terminal(s), application(s) and service(s) used.

Dependent on	UR 1.7 - Provision of a Universal Communications Identifier UR 2.3 - Generic control procedures UR 2.5 - Standardization of symbols, icons and pictograms
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 1.2 Seamless communication across networks and services

The independent development of different networks and services and their historical segregation has tended to make inter-network communication difficult if not impossible. Applications do exist to enable a user to send, for example, an email to a fax machine but typically it involves the user in significant effort. It is currently simpler for an originator to "experiment" until communication is established on one of the available networks than attempt to set up inter-network/inter-service communication.

For example, an originator first uses a fixed telephone to ring the recipient's fixed phone but gets a voice mailbox. The call is urgent so the originator clears down and rings a mobile number. Again there is no answer and this time they leave a message but for added peace of mind they now start up their home PC and send an urgent email to both the recipient's personal email address and their work email address. Altogether this is a time consuming process with unsatisfactory feedback. The use of translation agents (which could be part of the function of a Personal User Agent) within the network (e.g. voice to email, email to voice) would help to overcome this problem.

User requirement No UR 1.2
Users require seamless communication across networks and services.

At the present time, an originator has little control over outgoing communications other than by choice of terminal. In future the originator may want to specify the level of service required for a particular communication, specify what is to happen if desired communication cannot be established or assign a priority. As the number of possible options increases, the complexity for the user may increase. The user will need to be allowed to choose their own balance between increasing the options that they control and the reducing the complexity that a large number of choices can create.

Dependent on	UR 1.7 - Provision of a Universal Communications Identifier UR 2.3 - Generic control procedures UR 2.5 - Standardization of symbols, icons and pictograms
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 1.3 Increasing the options available to the originator

At the present time, an originator has little control over outgoing communications other than by choice of terminal. In future, the originator may want to specify the level of service required for a particular communication, specify what is to happen if the desired communication cannot be established or assign a priority. As the number of possible options increases, the complexity for the user may increase. The user will need to be allowed to choose their own balance between increasing the options that they control and reducing the complexity that a large number of choices can create.

User requirement No UR 1.3
The originator of a communication requires the ability to indicate to the system particular requirements relating to the outgoing communication.

Dependent on	SC 1.1 - Providing communication configuration status SC 1.2 - Editing the communication configuration SC 1.3 - Maintaining communication records SC 1.4 - Access to a personalized list of known UCIs SC 1.5 - Determining a UCI (if unknown) by means of a search process SC 1.6 - Selecting sending communication medium and characteristics SC1.7 - Providing cost information SC1.8 - Assign priority to communication when necessary SC 1.9 - Providing originator anonymity SC 1.10 - Using an alias SC 1.11 - Identifying the originator/recipient SC 1.12 - Verifying the identity of the originator/recipient SC 1.13 - Users identifying themselves SC 2.3 - Establishing contact where possible SC 2.4 - Taking account of local time SC 2.5 - Using the originators alphabet
Possible conflicts	UR 1.4 -The recipient requires the ability to control incoming communications

UR 1.4 Increasing the options available to the recipient

With the increasing number of communication options available to users it is becoming important to manage incoming communications effectively. In particular, a user may wish to divert incoming communications from one terminal to another depending on their own geographical location or the time/date. The recipient may also wish for the re-routing of communications to depend on the urgency of the call, whom it is from or some other attribute. Geographically determined re-routing of communications could be automated to varying degrees using GSM, GPS, AI techniques, polling, or other forms of presence detection.

User requirement No UR 1.4
The recipient requires the ability to control incoming communications.

Dependent on	SC 1.1 - Providing communication configuration status SC 1.2 - Editing the communication configuration SC 1.3 - Maintaining communication records SC 1.11 - Identifying the originator/recipient SC 1.12 - Verifying the identity of the originator/recipient SC 1.13 - Users identifying themselves SC 1.14 - Awareness of cost implications of routing/filtering SC 2.1 - User location monitoring SC 2.3 - Establishing contact where possible SC 2.8 - Barring/enabling incoming communications from specified originators
Possible conflicts	UR 1.3 - Increasing the options available to the originator

UR 1.5 Dealing with communications conflicts between originator and recipient

If the originator has specified particular attributes or conditions for a communication and the recipient has specified communication management criteria which conflict with those, then the system entities which represent originator and recipient within the network(s) should negotiate a mutually acceptable solution.

User requirement No UR 1.5
Users require that conflicts between the communication requirements of the originator and the recipient should be resolved, where possible, without their intervention.

Dependent on	UR 1.9 - User control of personal user agents SC 2.3 - Establishing contact where possible SC 2.4 - Taking account of local time SC 2.7 - Establishing the communication in the originator's preferred language
Possible conflicts	UR 3.1 - System performance

UR 1.6 Maintaining backward compatibility

Future architectures will provide users with increased control over the sending and receiving of communications. Taking full advantage of this increased functionality will almost certainly require sophisticated user interfaces. However, for the foreseeable future, a large number of terminals (principally telephones) will have limited or no ability to input alpha characters. It is important that these users are still able to use communications systems based on the new architectures, albeit with decreased functionality.

User requirement No UR 1.6 - Maintaining backward compatibility
Users may wish to use basic input devices such as a 12-button numeric keypad to obtain a basic level of service, even when using future architectures.

Dependent on	SC 4.3 - Number field of UCI
Possible conflicts	UR 1.7 - Provision of a Universal Communications Identifier SC 1.15 - User control of personal user agents

UR 1.7 Provision of a Universal Communications Identifier

Users now have access to a large and increasing number of methods of communicating with others. For example, the intended recipient of a communication could possess a pre-paid mobile, a home and work telephone, a fax and two email addresses each one having a different identifier. At any given time a person may not have access to the terminal needed to receive an incoming communication. Also, determining the best communication strategy to reach someone can easily become a non-trivial task. The obvious solution is a communications architecture which supports a single universal identifier associated with a person, role or organization instead of a terminal. The requirements associated with this identifier are described by User Requirements UR3.1 to UR3.8.

User Requirement No UR 1.7 - Provision of a Universal Communications Identifier
Users require a universal identifier which meets as far as possible the requirements outlined in Requirements UR3.1 to UR3.8.

Dependent on	UR 3.1 - Uniqueness UR 3.2 - Memorability UR 3.3 - Length UR 3.4 - Persistence UR 3.5 - Terminal Independence UR 3.6 - Robustness UR 3.7 - Meaningfulness UR 3.8 - Additional Information
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 1.8 Trust in the system

Trust in a communications system is clearly dependent on many issues other than technical ones. A user's trust in a communications system will be influenced not only by the security mechanisms within the system but by political and psychological factors as well.

However, trust can be maximized by providing "appropriate" levels of security. A typical user may not be concerned about the integrity of 95 % of their communications and supplying checks and verifications on these would be inefficient with respect to system performance and frustrating for the user. But for the remaining 5 % the user may require these features and needs to have confidence that in these cases appropriate security is in place.

User requirement No UR 1.8 - Trust in the system
To have trust in a communications system, users require an appropriate level of security to be provided and when necessary an assurance of the integrity of the communication and the identity of the person they are communicating with.

Dependent on	SC 3.1 - Provision/non-provision of location information SC 3.2 - Provision/non-provision of availability information SC 3.3 - Providing confidentiality/privacy of stored personal data SC 3.4 - Providing confidentiality/privacy of communications SC 3.5 - Assuring identity SC 3.6 - Providing integrity SC 3.7 - Providing accountability
Possible conflicts	SC 1.15 - User control of personal user agents

UR 1.9 Appropriate level of privacy

Privacy is defined as the ability of the user to choose who knows their UCI and under what circumstances and from whom they can accept incoming communications. Users will wish to have the freedom to determine who is able to gain access to their UCI (via such mechanisms as UCI searches). They will also wish to have full control over who is able to communicate with them, when and by what means.

User requirement No UR1.9 - Appropriate level of privacy
Users will require different levels of privacy dependant on their individual needs.

Dependent on	SC 3.1 - Provision/non-provision of location information SC 3.2 - Provision/non-provision of availability information SC 3.3 - Providing confidentiality/privacy of stored personal data SC 3.4 - Providing confidentiality/privacy of communications SC 3.5 - Assuring identity SC 3.6 - Providing integrity
Possible conflicts	SC 1.15 - User control of personal user agents SC 1.5 - Determining a UCI (if unknown) by a means of a search process SC 2.3 - Establishing contact where possible

B.3 Human factors requirements

UR 2.1 System performance

The effect of system response times on the user perceptions of communication and information systems is well researched and documented. Users have expectations regarding call set up times (post dialling delay), terminal processing times and so on. The network architecture proposed in the present document requires considerable processing to be undertaken before a communication is established and so due consideration will need to be given to ensure that acceptable performance levels are delivered.

User requirement UR 2.1 - System performance
When retrieving information and setting up communications, users require that system response times meet accepted HF recommendations and standards.

Dependent on	UR 1.2 - Seamless communication across networks and services
Possible conflicts	UR 1.5 - Dealing with communications conflicts between originator and recipient UR 1.6 - Maintaining backward compatibility

UR 2.2 Ease of use

Use of the UCI in an advanced communications architecture assumes that users will be provided with enhanced control over their communication environment. Where users are given control, a user interface must be provided. An effective user interface can make controlling the communication environment easy and pleasurable but a poor user interface can mean that users fail to effectively control their environment and that they become frustrated and cease to use the facilities provided. User interfaces supporting the proposed architecture should conform to best practice.

The following areas are highlighted as those in which particular care is needed to ensure that the overall environment is usable.

- Communications set-up
- Incoming communications information

- Communications management
- Directory search strategies
- Verification
- Presentation of UCI (on paper)
- Presentation of communications history
- The communication set-up procedure including:
  - Users manipulation
  - System performance

  These should be comparable in timing and feel to today's communication set-up.

All of these issues are being addressed in the work of STF200.

User Requirement No UR 2.2 - Ease of use
All aspects of communication including initiation of a specific communication, access to records, setting up and editing communications configurations should comply with usability best practice and be as intuitive as possible.

Dependent on	UR 2.1 - System performance UR 2.3 - Generic control procedures UR 2.4 - Providing feedback to the user UR 2.5 - Standardization of symbols, icons and pictograms UR 2.6 - Accessibility
Possible conflicts	UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient UR 1.6 - Maintaining backward compatibility

UR 2.3 Generic control procedures

Standardization of user control procedures can be seen as something which stifles creativity and limits commercial advantage. However, many service providers now agree that defining a base level set of protocols and procedures which are generic to all terminals applications and services increases the usability of the systems and therefore customer acceptance and uptake.

By using such standards, a minimum level of usability can be achieved within and between telecommunication services by the acceptance of well researched minimum user control procedures. The expected format of such procedures would define a minimum sequence of indications and controls necessary to enable the user to make use of a service. The procedures would not define the format or substance of the controls or indications and would not preclude other enhanced procedures from being provided, but they would ensure that a user could access and control a service irrespective of the terminal or network being used.

User requirement UR 2.3 - Generic control procedures
Users will require that the basic protocols and procedures used to set up communications are standardized across terminals, applications and services.

Dependent on	UR 1.1 - Unifying the control of communications UR 1.2 - Seamless communication across networks and services
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 2.4 Providing feedback to the user

One of the most important determinants of a usable system is the provision of feedback to the user. The architectures being developed to support the UCI have the potential to provide complex communications configurations to users and it is essential to provide continuous feedback regarding system status and the options available if the user is to exploit the full potential of the system.

User requirement UR 2.4 - Providing feedback to the user
Feedback should be given on status and options available to the user whenever feasible.

Supports	UR 1.2 - Seamless communication across networks and services
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 2.5 Standardization of symbols, icons and pictograms

As users may well interact with the system on a variety of input devices on different applications, it is critical that icons, symbols and pictograms are standardized across terminals, applications and services, and are designed as a coherent, logical set. If this issue is left to market forces there is a danger of a variety of symbols being developed for the same identity, function or action. This could compromise the uptake of the service.

User requirement UR 2.5 - Standardization of symbols, icons and pictograms
Users require a consistent coherent set of symbols relating to UCI usage that can be used across terminals, applications and services.

Supports	UR 1.2 - Seamless communication across networks and services
Possible conflicts	UR 1.6 - Maintaining backward compatibility

UR 2.6 Accessibility

"All new telecommunication facilities and services should be accessible to all (users)" (Telecommunications Charter COST219). The needs of children, older people and people with disabilities should be taken into account in the design of any new telecommunication equipment or service. Any new architecture should be designed for the widest possible market and the services and applications that use such an architecture should adequately support relevant special terminal functions so that all users can experience end-to-end service.

The use of PUAs in an architecture enables communications to be configured taking any special requirements of a user into consideration.

User Requirement No UR 2.6 - Accessibility
Children, elderly people and disabled users will require access to the full functionality of the system and the design of all users interfaces should take this into account. PUAs should be aware of capabilities of their users and manage communications accordingly.

Dependent on	UR 1.3 - Increasing the options available to the originator UR 1.4 - Increasing the options available to the recipient
Possible conflicts	UR 1.1 - Unifying the control of communications

Annex C (informative): Standards Bodies related to UCI Technical Requirements

It was always intended that the UCI architecture should, wherever possible, be built upon existing and emerging standards. For this reason it is important to identify those standards activities that relate to the various technical requirements described in clause 8. Clauses C.1 to C.4 list the standards activities that relate to each of the UCI Technical Requirements.

C.1 Personal User Agent Technical Requirements

Table C.1 shows those standards activities that relate to the PUA Technical Requirements. The numbers used as the headings of the table column are the numbers of the technical requirements used in table 1 in clause 8.

Table C.1: Standards bodies related the PUA Technical Requirements

	Technical Requirements																																	
Standards bodies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
3GPP OSA, PARLAY, JAIN™,SPAN 14 (SPAR)			X			X	X													X	X						X	X				X		
IETF IMPP, PAM FORUM, 3GPP Presence	X	X								X	X		X	X									X											
SMARTCARD Charter, ETSI E-Commerce										X	X						X	X	X					X										X
TIPHON								X	X			X																						
SPAN 11										X	X									X	X								X	X				
ITU SG2										X	X									X	X								X	X				
ITU SG7, IETF IPSec										X	X													X	X	X	X	X				X		X
3GPP VHE; GUP;	X	X													X																			
IETF ENUM																														X				
IETF VCARD										X	X						X	X	X															
FIPA									X				X	X																				
TC HF	X	X							X	X	X				X														X	X	X		X	
ISO SC18 WG9, CEN																																		
ITU SG13												X																						
SyncML				X																									X	X	X			
ITU SG4			X					X	X			X								X	X						X	X						
SPAN12/13			X																															
3GPP LCS													X									X												
IETF LDAP					X																													
3GPP TSG T																	X																	
ETSI TC AT																	X																	
Nobody																X																		

Due to the very wide range of potential capabilities of the PUA, there is a very broad range of standards bodies that relate to the PUA Technical Requirements. The standards body that most specifically addresses PUA issues, as it relates strongly to PUA to PUA interaction, are the (potential) standards of FIPA. Another activity that is particularly relevant to many of the core PUA capabilities is the 3GPP work on Generic User Profile. Also, all of the organizations addressing Smart Cards are relevant to PUA Technical Requirements as Smart Cards may be involved in the registration of users with their PUAs.

C.2 Service Agent

Table C.2 shows those standards activities that relate to the SA Technical Requirements. The numbers used as the headings of the table column are the numbers of the technical requirements used in table 2 in clause 8.

Table C.2: Standards bodies related to SA Technical Requirements

	Technical Requirements												
Standards bodies	1	2	3	4	5	6	7	8	9	10	11	12	13
3GPP OSA, PARLAY, JAIN™,SPAN 14 (SPAR)	X	X	X	X	X	X	X		X		X	X	X
IETF IMPP, PAM FORUM, 3GPP Presence					X	X							
TIPHON		X	X				X						
SPAN 11 ITU SG2				X									
ITU SG7, IETS IPSec				X			X		X				
ITU SG13		X											
SyncML											X	X	X
ITU SG4	X	X	X	X									
SPAN12/13	X												
3GPP LCS					X								
Not applicable								X		X			

As the SA is the gateway to a network or service, it will be important to select protocols and interfaces that are generally accepted by network and service providers as a legitimate method of 3rd party access. For this reason, the most significant group of standards bodies that are working in areas related to SA Technical Requirements are the group in the first row of table C.2 that cover such access.

C.3 Terminals and end-user applications

Table C.3 shows those standards activities that relate to the technical requirements related to terminals and end-user applications. The numbers used as the headings of the table column are the numbers of the Technical requirements used in tables 3 and 4 in clause 8.

Table C.3: Standards bodies related to terminal and end-user application Technical Requirements

	Technical Requirements													
	Terminals										Applications			
Standards bodies	1	2	3	4	5	6	7	8	9	10	1	2	3	4
3GPP OSA, PARLAY, JAIN™,SPAN 14 (SPAR)												X		
IETF IMPP, PAM FORUM, 3GPP Presence	X	X									X			
SMARTCARD Charter, ETSI E-Commerce											X	X	X	X
TIPHON						X								
SPAN 11 ITU SG2											X	X		
ITU SG7, IETS IPSec											X	X		
3GPP VHE; GUP	X	X												
IETF VCARD											X	X	X	X
TC HF	X	X	X	X	X	X	X	X		X	X	X	X	X
SyncML	X		X											
IETF LDAP				X										
3GPP TSG T, ETSI TC AT	X	X	X	X	X	X	X	X	X	X				

The most significant standards bodies in the terminal and end-user application areas are:

- ETSI TC HF, ITU-T SG2 that cover Human Factors issues;
- 3GPP TSG T and ETSI TC AT that cover terminal issues.

C.4 UCI and identification verifiers

Table C.4 shows those standards activities that relate to both the UCI and Identification Verifiers Technical Requirements. The numbers used as the headings of the table column are the numbers of the technical requirements used in table 5 in clause 8.

Table C.4: Standards bodies related to identification verifier Technical Requirements

	Technical Requirement
Standards bodies	1
SMARTCARD Charter, ETSI E-Commerce	X
ITU SG7, IETS IPSec	X
IETF VCARD	X
TC HF	X

The most significant group of standards activities in this area are the Smart Card Charter and ETSI E-Commerce activities that cover smartcards and secure communications using Smart Cards.

Annex D (informative): Security Mechanisms

Meeting the objectives with a policy and set of functions and countermeasures is not enough. Security is not a problem that is solved once and then remains solved. There is a process to be met:

- Monitor;
- Modify;
- Maintain.

Computer and communications systems security flaws are inevitable.

Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. In order to reduce the risk it is important to know what risk is acceptable and to maintain security levels to meet this level of risk. In this context a security protocol or algorithm is a product.

Real security is hard, slow, and expensive, both to design and to implement. Security does not have to be perfect, but the risks have to be manageable, and more importantly known. This clause considers the threats that can be used to exploit IP telephony systems.

Security is old, the security industry thinks of countermeasures not as ways to counter threats, but as ways to reduce risk. This distinction is enormous. Avoiding threats is black and white: either you avoid the threat, or you do not. Reducing risk is continuous: there is some amount of risk you can accept, and some amount you cannot.

D.1 Public, Private and Secret Keys

Cryptography, the mathematics and science of secrecy, has a long and chequered history. Wars have been won and lost as a result of the skill of cryptographers to make things secret or by the skills of cryptanalysts to break secrets.

The encryption toolkit consists of 2 elements: a lock and a key. The lock is what we tend to consider nowadays as the algorithm. We make the general assumption today that algorithms are public knowledge whilst the secrecy is provided by the key.

Of itself cryptography can be considered symmetric or asymmetric. The former case has the communicating parties sharing a secret (the key). Asymmetric encryption arose from a conceptual problem posed by Ellis in the late 1960s: Can we exchange encrypted data without exchanging/sharing secrets? This problem was solvable in theory (i.e. existence theory says that a solution is possible without identifying the solution) and is made possible if the recipient is in the loop of the encipherment.

If a function can be made "one-way" for most cases but can be reversible in special circumstances then it is possible to encrypt using the one-way function in its normal mode, and decrypt by reversing the function in special circumstances. The two paths use separate keys, one public (to use the one-way function in its normal mode), one private (to use the one-way function in its special reversible mode). As it is computationally difficult to find the private key even knowing the algorithm and the public key it is possible to make the public key not secret. This solves the Ellis conundrum of non-secret encryption as the public key can be distributed without fear of secrets being intercepted (i.e. decrypted).

D.1.1 Symmetric key advantages and disadvantages

It is not the key that has advantages but the algorithm that uses it. Symmetric keys are generally quite short (80 bits is state of the art today). Because the keys are short the algorithms tend to be high speed and suited to real time communication as can be seen in their adoption by GSM, TETRA and similar systems.

The biggest disadvantage of symmetric key systems is in maintaining symmetry. By symmetry we mean that only 2 parties have knowledge of the key. This is fine where users only have to communicate with one party. However in practice communication in the public domain is between many parties and these each have to be secured. Symmetric methods can be maintained in such an event with clustering (A talks to B, who then talks on A's behalf to C). This model is vulnerable as the key material is concentrated at the cluster points.

Is symmetric key encryption secure? Yes, although how secure depends on key length and algorithm.

D.1.2 Asymmetric key advantages and disadvantages

Asymmetric encryption is much better known as public key encryption and works on the basis of a lock being able to be opened by 2 different keys. Every user creates a key pair and keeps one of them private (i.e. known only to that user, not shared). If a user wishes to receive encrypted data from any party he offers that party his public key.

There are a lot of management issues regarding public/private key encryption. The greatest problem is knowing that the public key being offered is the partner of a known private key. This is what a lot of organizations such as VeriSign are in business to sort out. The level of trust you have in the ownership of a public key determines to a large extent to what degree the system is considered secure. If there is a low level of trust in the information about a key that is given to you then the plausibility of the security of the network is similarly low. It is important to be able to determine if a public key "belongs" to someone. This is particularly important for e-commerce as a transaction is secured with the vendor's public key and can only be decrypted by that vendor's private key. If you were to be falsely assured that the key belonged to a trusted vendor but was in fact only a masquerade you could securely deliver your credentials to a thief.

Is public key encryption secure? Yes, mathematically with today's known difficulties in reversing one-way functions (the majority of current one-way functions are based upon the difficulty in factoring large numbers), public key encryption forms offer adequate security.

D.1.3 General encryption management problems

Encryption fails mostly because the management fails. If a public key is compromised it is generally compromised because the ownership has been falsely assured e.g. a key purporting to be paired and owned by A but in fact being used by B allows B to masquerade as A. This has happened.

Symmetric key encryption tends to fail when the key is shared between more than 2 parties. Every additional party raises the risk of the secret key becoming public knowledge and hence offering no security at all. This has of course happened (e.g. device copy protection ware).

What things like IKE [4], ISAKMP [5] [7], SKEME, OAKLEY and similar recommendations offer is a systematic way or guide to maintaining security and in particular managing keys.

D.1.4 Can encryption be perfect?

No. Given enough time any cipher-text can be broken. It may take many years (hundreds, thousands). The goal generally of encryption is to make the plain-text secure for a reasonable period and in large part that determines the key length (generally we need to increase the symmetric key length (or its equivalent) by 1 to 2 bits per year to maintain a secure period (i.e. time to recover plain text using brute force from a cipher text)). If the algorithm is poor it may introduce patterns into the cipher text that cut the time to break it but most public domain algorithms have been tested and not found wanting in this area.

D.2 Internet Key Exchange (IKE)

D.2.1 Overview

The Internet Security Association and Key Management Protocol [5] provides frameworks for authentication and key exchange but does not define them. There are a number of methods for key exchange described by RFCs (Oakley [6] et al). What IKE [4] does is merge and simplify two of the key exchange methods (Oakley [6] and SKEME [8]) into one for use with ISAKMP [5] [7] and for IPsec's AH and ESP.

D.2.2 What IKE achieves

IKE [4] is a hybrid protocol whose purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner. The intended operational scenarios for IKE [4] are for negotiating virtual private networks (VPNs) and also for providing a remote user from a remote site (whose IP address need not be known beforehand) access to a secure host or network. In addition IKE [4] supports a mode called client negotiation in which the key negotiating parties are not the endpoints for which security association negotiation is taking place. When used in client mode, the identities of the end parties remain hidden.

D.2.3 IKE in UCI

IKE [4] has possible use in UCI as part of the implementation framework but at this time, preceding the outcome of a threat analysis, no recommendations can be made as to its application.

D.3 Digital Signature and Signature in General

A signature is one method of proof in document exchange. Generally a user lodges a sample signature with some agency (for example a bank) and whenever a document is offered to the bank purporting to be signed the current and stored signatures are compared. If they are the same then the document can generally be supposed to have been signed by the person who lodged the sample.

A digital signature is primarily a legal support device intended to offer documents sent/stored/offered digitally the same legal meaning as paper copies with a signature. In practice there are many detractors to digital signature as the document being signed is not physically signed by the user but by the user's machine. It is therefore possible to use someone else's machine and to sign documents from the other person as the signature is often machine stored.

There is a very large mechanism of officers and agents in digital signature to support the legal framework and much of the digital signature development has been on the legal frameworks in which a digital signature is applicable.

http://www.etsi.org/sec/el-sign.htm

This often uses a form of public key encryption but with a different intent. The intention is to be able to take a document (as a generalized form of data structure), process it in such a way that it can be detected if any changes have been made by creating a cryptographic digest, and to use the "signer's" private key to create the digest. Any party with the signer's public key can verify that the digest shows the document was unmodified from the state at which the digest was created.

D.3.1 Digital signature and UCI

At this time UCI may be "signed" in its store although the effect of this on storage and recovery times needs further investigation.

Annex E (informative): Security risk assessment

In this annex the results and analysis of a security risk assessment using numeric methods for the UCI system is presented.

There are two phases in risk assessment:

- Initial risk assessment, which is conducted before security features applied; and
- Final assessment, which is conducted with the identified (required) security features applied.

E.1 Initial risk assessment

The results of the initial risk assessment for UCI system are shown in table E.1.

Table E.1: Initial Risk Assessment

Threat Description	Impact Value (I)	Likelihood of Occurrence (O)	Exposure Factor (I X O)	Rank of Threat
T1.Eavesdropping of IFa	3	3	9	**Critical**
T2. Eavesdropping of Ifb	2	2	4	**Major**
T3. Eavesdropping of IFc	2	3	6	**Critical**
T4. Eavesdropping of IFd	3	2	6	**Critical**
T5. Eavesdropping of IFe	2	2	4	**Major**
T6. Masquerade of a user	3	3	9	**Critical**
T7. Masquerade of a PUA	3	1	3	**Minor**
T8. Masquerade of an SA	2	1	2	**Minor**
T9. Replay of IFa	3	3	9	**Critical**
T10. Replay of Ifb	2	1	2	**Minor**
T11. Replay of IFc	2	3	6	**Critical**
T12. Replay of IFd	2	1	2	**Minor**
T13. Replay of IFe	2	1	2	**Minor**
T14. Modification of IFa	3	1	3	**Major**
T15. Modification of Ifb	2	1	2	**Minor**
T16. Modification of IFc	2	1	2	**Minor**
T17. Modification of IFd	3	1	3	**Major**
T18. Modification of IFe	2	1	2	**Minor**
T19. Unauthorized access to user profile	3	2	6	**Critical**
T20. Stalking	3	3	9	**Critical**
T21. Denial of PUA service	3	2	6	**Critical**
T22. Denial of SA service	2	2	4	**Major**

In table E.1, Impact Value and Likelihood of Occurrence take values from the value set {1, 2, 3}. Here, 1 means low, 2 means medium, and 3 means high. Exposure Factor takes value from value set {1, 2, 3, 4, 6, 9}. According to the Exposure value, threats are classified as critical (Exposure Value = 9 or 6), major (Exposure Value = 3 or 4), and minor (Exposure Value = 1 or 2). When specifying security features to counter threats, only critical threats and major threats will be considered.

E.2 Final risk assessment

To evaluate the effectiveness of proposed security features (described in clause 13.7), a final risk assessment was conducted. The results of the final risk assessment are listed in table E.2. In table E.2, the Likelihood of Occurrence of a critical or major threat is reduced to the Likelihood of Occurrence of the Residual Threat. If the security features are designed properly, all residual threats shall be minor.

Table E.2: Final Risk Assessment

Threat Description	Rank of Threat	Security Features to Counter Threat	Impact Value (I)	Likelihood of Occurrence for the Residual Threat (O)	Exposure Factor for the Residual Threat (I X O)	Rank of the Residual Threat
T1. Eavesdropping of IFa	Critical	F3	3	1	3	Minor
T2. Eavesdropping of IFb	Major	F4	2	1	2	Minor
T3. Eavesdropping of IFc	Critical	F5	2	1	2	Minor
T4. Eavesdropping of IFd	Critical	F6	3	1	3	Minor
T5. Eavesdropping of IFe	Major	F7	2	1	2	Minor
T6. Masquerade of a user	Critical	F1	3	1	3	Minor
T7. Masquerade of a PUA	Minor		3	1	3	Minor
T8. Masquerade of an SA	Minor		2	1	2	Minor
T9. Replay of IFa	Critical	F2	3	1	3	Minor
T10. Replay of Ifb	Minor		2	1	2	Minor
T11. Replay of IFc	Critical	F2	2	1	2	Minor
T12. Replay of IFd	Minor		2	1	2	Minor
T13. Replay of IFe	Minor		2	1	2	Minor
T14. Modification of IFa	Major	F8	3	1	3	Minor
T15. Modification of Ifb	Minor		2	1	2	Minor
T16. Modification of IFc	Minor		2	1	2	Minor
T17. Modification of IFd	Major	F9	3	1	3	Minor
T18. Modification of IFe	Minor		3	1	3	Minor
T19. Unauthorized access to user profile	Critical	F1, F12	2	1	2	Minor
T20. Stalking	Critical	F1, F2, F3, F4, F5, F6, F13	3	1	3	Minor
T21. Denial of PUA service	Critical	F10	3	1	3	Minor
T22. Denial of SA service	Major	F11	2	1	3	Minor

From the rightmost column of table E.2, it is known that the security features proposed in clause 13.7 are effective to reduce the risk to the acceptable level. This means the resulting UCI system addresses those risks and may be considered resistant to attack in those areas.

Annex F (informative): Comparison of the UCI approach with ENUM

F.1 ENUM

The scope of ENUM as stated in IETF RFC 2916 "E.164 number and DNS" [2] is:

"This document discusses the use of the Domain Name System (DNS) for storage of E.164 numbers. More specifically, how DNS can be used for identifying available services connected to one E.164 number. Routing of the actual connection using the service selected using these methods is not discussed."

It was stated in draft-ietf-enum-operation-02 "ENUM Service Reference Model" that, "Use of the ENUM system to implement time-of-day and other highly dynamic services is discouraged. Where such a service is desired, it is recommended that itself be implemented as part of a service indicated by the service records."

The "client" representing a communication originator uses the E.164 number associated with the receiver of a communication and receives from DNS a NAPTR record listing a number of available services with their associated service identifiers (e.g. sip: + Joe@company.com, tel: +4689761234, mailto:paf@swip.net). Associated with each of the items in the list are indications of the order in which the client should process the NAPTR records.

F.2 UCI

The Universal Communications Identifier (UCI) [1] is also used to identify people associated with access to a range of available services. There are 3 options as to how the service and the associated destination identifier are chosen:

a) When the UCI is fully used, the choice of the service and associated identifier of the communication receiver is a matter of negotiation between the Personal User Agents (PUAs) of the originator and the receiver of the communication. A key benefit of the use of the UCI compared with ENUM is that it allows the **recipients** of communications, not the originators of the communication, to have the final say about the way that they wish to receive a specific communication.

b) When the originator of the communication is unable to identify themselves, the PUA of the recipient of the communication negotiates with the Service Agent (SA) associated with the service the originator is using. This negotiation determines the (matching) service and associated identifier that the recipient will choose to use for the communication (e.g. the PUA of the recipient gets to choose which of the recipient's many telephones will be used to receive the incoming telephone call).

c) When the receiver of the communication has no UCI, the PUA of the originator may be involved in the communication. The service and destination identifier are not negotiable except where the receiver is an ENUM subscriber, in which case the PUA can be involved in processing the NAPTR record.

F.3 Similarities between ENUM and UCI

Both ENUM and UCI propose the use of an E.164 number as the identifier (or part of the identifier for UCI) used to negotiate a communication. Both proposals assume that the E.164 number can allow the originator of a communication to communicate with the receiver using one of a number of potential services that both the originator and receiver have available.

F.4 Differences between ENUM and UCI

In ENUM, the NAPTR record contains a list of all the services and identifiers that the user wishes to declare as potential means to be contacted. Draft-ietf-enum-operation-02.txt makes it clear that it is not intended that this information should be dynamically changed (due to DNS propagation delays). It is therefore not feasible for the person with an ENUM number to change their NAPTR record every time that their mobile is switched on and off, or every time they leave their home. It is certainly not possible for the ENUM user to change the NAPTR record according to the recognized identity of the person accessing the NAPTR record. Such options can only be achieved with ENUM if the NAPTR record points to a service that performs these dynamic functions.

The UCI enables a receiver to opt for a different communication service to be used according to the identity of each communication originator. It also make it very easy to dynamically change the preferred means of communication according to the status of the relevant services (e.g. mobile switched on or off, currently unable to read email) according to the time of day, or according to some other set of event or time driven rules.

In some cases the UCI can also provide the recipient with an indication of the identity of the originator. This can be particularly useful if the recipient wishes to receive communications of particular importance or urgency.

Finally, the current plans for UCI enable the receiver of the communication to receive communications across **all** of their available services without revealing the service specific identifier that is used to reach them on **any** of their services. This provides the receiver of a communication complete control of their **privacy** whilst still maximising their **reachability**.

In contrast, in ENUM, the recipient of a communication only has the option of adding a potential communication service and its associated identifier to the NAPTR record or not adding it (thereby making it invisible to ENUM). ENUM provides the user no means to selectively add (or remove) services and identifiers to (or from) the NAPTR record dependant on the identity of the communication originator or according to the current dynamic status of the recipient's services.

F.5 Summary

UCI facilitates far more features than a basic ENUM service. A basic ENUM service provides no privacy protection for the user's service specific identifiers (e.g. telephone numbers, email addresses, etc.). Indeed, a basic ENUM service presents the user with the current classic privacy protection dilemmas:

- the user must make their service specific identifiers public (in their NAPTR record) to enable anyone to communicate with them using the relevant service;
- once an identifier is listed in the NAPTR record it can be accessed by anyone (any client) and can then be used to contact the owner of the identifier at any time whether the identifier owner wishes to receive communications via that service or not;
- the only way not to make an identifier public is not to list it in the NAPTR record, but this makes the person totally uncontactable via the related service by anyone using ENUM.

In addition, ENUM is unable to provide any of the dynamic behaviour implicit in a UCI-based system (e.g. responding differently according to the identity of the originator of a single communication).

The "service" referred to in the quote from "Draft-ietf-enum-operation-02" in clause F.2 above could be the same service being defined in STF180 to support UCI. In this case UCI is effectively providing a very major extension to ENUM. This means that UCI could be built as an extension of ENUM, but UCI does not depend on ENUM. In fact it may be preferable and more efficient to have a method of directly translating between the numeric element of a UCI and the actual address of a PUA that does not rely on the more generic ENUM.

History

Document history		
V1.1.1	July 2002	Membership Approval Procedure MV 20020913: 2002-07-16 to 2002-09-13