# ETSI EG 201 940 V1.1.1 (2001-04)

*ETSI Guide*

## Human Factors (HF);
## User identification solutions in converging networks

Reference

DEG/HF-00011

Keywords

addressing, multimedia, network, telephony

***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://www.etsi.org/tb/status/

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

***Copyright Notification***

# Contents

# Intellectual Property Rights

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

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).

# Introduction

**Executive summary**

Currently, users of communications systems are presented with a large and increasing number of methods of establishing a communication with a potential receiver. For example, the intended receiver 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. Many of these terminals may not be accessible by the receiver at any given time. Determining a communication strategy to contact an intended receiver can easily become a non-trivial task. Not establishing a successful communication can result in unsuccessful attempts to set up communications which leads to:

a) Decreased revenue for the Service Provider because of fewer communications;

b) User frustration and dissatisfaction with the Service Provider leading to:

  - further decreases in usage and therefore reduced revenue; and

  - reduced customer loyalty.

Annexes to the document examine the current and evolving communications environment. These identify some of the problems faced, or that will be faced, by a user trying to use and manage an environment which consists of a multitude of services and networks each with different identifiers. The present document looks at the issues involved in the creation of a universal identifier, which would identify an intended receiver and not a terminal. The present document refers to this identifier as a Universal Communications Identifier (UCI).

In order to propose a new identifier, it is necessary to understand the user requirements which will underpin it. The approach of the present document is to determine those user requirements in a hierarchical way. Clause 5 defines nine top-level requirements relating to generic communications needs.

Refining these requirements, the present document makes assumptions about the types of networks in which a UCI might be used. For instance, a common theme amongst all emerging architectures is the concept of a software entity or entities that manages the user's communications (a "Personal User Agent" or PUA). Subsequently, a further twenty user requirements (clause 6) relating to communication control are proposed. These support the generic requirements of clause 5.

The final ten user requirements (clause 7) relate specifically to the identifier which would be needed in such a communications environment. The set of ten user requirements thus obtained provide the criteria against which any proposed new UCI (or solutions not involving new identifiers) must be compared. Three of these user requirements relating to the identifier have been designated as possessing **essential** attributes:

- uniqueness - identifying one person, organization or role in an organization amongst all other accessible people, organizations and roles;

- stability - not changing with change of Service Providers, user's address etc.;
- user-friendliness - being as short, meaningful and memorable as possible.

Three currently used identifiers, when evaluated against the ten identifier requirements, are shown to have serious shortcomings particularly when assessed against the essential requirements. Four potential solutions which are proposed, two of which cope with multiple identifiers without proposing a new identifier. These four proposals are rejected because they fail to meet sufficient of the user requirements.

A solution is proposed which performs best against the test criteria (clause 10). It is a new identifier of the form:

This consists of:

a) an alphabetic label that is the name by which the person or organization usually wishes to be known. This label would be used to access the complete UCI from the user's address book, and would be used to show who a communication was from;

b) a numeric string that is globally unique. Under most circumstances it would not be necessary for a user to memorize or enter this string as it would be "captured" from incoming communications, business cards or from a directory service, and stored in an address book function;

c) an additional part of the label which imparts extra information in the form of flags. These flags would not be directly visible but could indicate to the receiver's PUA whether the communication was from a business source or a private individual, and whether alphabetic label was a real name or an alias. This information could be used to make filtering/routing decisions for incoming communications or could be passed on to the receiver for information.

Such an identifier satisfies the, seemingly, incompatible requirements of "uniqueness" and "user-friendliness" by having a unique core to the identifier with a user-friendly "attachment". In essence, it identifies not a terminal but the software entity (PUA) which represents a person, organization or role in an organization) and which has knowledge of what terminals are available to that party. This gives it "stability" as it does not need to change every time the services or terminals change.

To address the requirements of trust and security, it is suggested that each such UCI must be allocated by a "trusted" third party and be tamper-proof. This third party would allocate and register the UCI and make it, and additional data to aid searching, available to directory search entities, (but only if the owner allowed it to be).

The UCI is thus part of a handling system which is conceived very much as an "overlay" to a multitude of networks and services. Such a system would normally require that the PUAs of sender and receiver "negotiate" before a communication is set up.

These and other implications of implementing such a UCI with future network architectures are discussed:

- Allocation/registration of UCIs;
- Security of UCIs;
- Usage of the UCI;
- Negotiation between PUAs;
- Migration issues including backward compatibility;
- Directory structures.

Universal adoption of such a system would require standards in several areas. Naturally, the format of the UCI itself will require standardization but additionally, standardization covering PUA intercommunication and directory structures will be needed.

Although it will be an overlay system, the setting up of a UCI/PUA based communications architecture will be a large undertaking. However, the rewards, in terms of increased user satisfaction and increased network usage and revenue would also be great. The UCI derived as a result of this study offers a practical way forward to a very effective way of managing communications in an increasingly complex environment.

# 1 Scope

The areas covered by the present document are:

1) End-user requirements of end-user identification solutions are described. In particular the following are covered:

   - the end-user requirements involved in establishing person-to-person communication using whatever means (fixed or mobile telephone, e-mail, SMS…) that are chosen;
   - the end-user requirements of dealing with incoming communications, in relation to end-user identity issues;
   - the end-user requirements involved in setting up and configuring a system to deal with incoming and outgoing communications.

2) A number of end-user identification solutions that address all person-to-person electronic communication means are described. High-level potential solutions and not detailed, specific, technical solutions are discussed.

3) Issues involved in providing these solutions are described. Specifically:

   - the issues involved in configuring the environment to make and receive communications;
   - the issues involved in requesting and using the identity of the party with whom a sender wishes to communicate;
   - the issues involved in dealing with incoming communications.

4) An analysis of how a preferred universal solution for end-user communications identification can be effectively introduced into existing networks and services.

Only potential solutions that require little or no changes to the way in which current numbering and identification mechanisms within networks and the Internet currently work are considered in the present document. Solutions that require significant re-engineering of existing networks or of the Internet are avoided. Although not specifically addressed, an attempt has been made to take into account commercial issues in the formulation of solutions.

The present document shows how enhancements to terminals and to peripheral elements of networks can significantly enhance the benefits derived from the proposed solution. Multicast and broadcast are considered to be outside the person-to-person scope. It is also possible that the same identification solution might be used to identify services and various non-human entities. Consideration of these alternative uses for the identification solutions are outside the scope of the present document.

# 2 References

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

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

[1] ETSI EG 201 795: "Human Factors (HF); Issues concerning user identification in future telecommunications systems".

[2] ITU-T Recommendation X.400/F.400 (1996): "Message handling system and service overview".

[3] ITU-T Recommendation X.500 (1997) | ISO/IEC 9594-1 (1997): " Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

[4] ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2 (1997): "Information technology - Open Systems Interconnection - The Directory: Models".

[5] ITU-T Recommendation X.509 (1997): "Information technology - Open Systems Interconnection - The Directory: Authentication framework".

[6] ITU-T Recommendation X.511 (1997) | ISO/IEC 9594-3 (1997): "Information technology - Open Systems Interconnection - The Directory: Abstract service definition".

[7] ITU-T Recommendation X.800 (1991): "Security Architecture for Open Systems Interconnection for CCITT applications".

[8] IETF RFC 1737: "Functional Requirements for Uniform Resource Names".

[9] IETF RFC 2426: "vCard MIME Directory Profile".

[10] ITU-T Recommendation E.123 (1988): "Notation for national and international telephone numbers".

[11] RFC 1034 (November 1987): "Domain names - concepts and facilities".

[12] RFC 1630 (June 1994): "Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web".

[13] RFC 822 (August 1982): "Standard for the format of ARPA internet text messages".

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**alias, alias name:** alternative name for an object (individual) [3]. an individual may have many different aliases.

**authentication:** provision of assurance of the claimed identity of an entity (see "Context and Goals for Common Name Resolution", annex G)

**authorization:** granting of rights to perform some activity to some entity, human agent or process until revoked

**Calling Line Identity (CLI):** service which allows the display on the receiving terminal of the number from which the call originates

**Calling Name Identity (CNI):** service which allows the display on the receiving terminal of a name assigned to the originating line

**chunking:** breaking up the presentation of a long number in to smaller, more memorable, groups (e.g. 0123 94 42 67)

**certification authority:** authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys

**Golden Number:** number having some mnemonic property such as repeated sequences of memorable digits (e.g. 0800-800 800) or numbers which map to a meaningful word on a telephone keypad (e.g. 0800-43789 can be mapped to 0800-HERTZ)

**identification:** process of establishing the identity of an object or person

**identity:** data or information (*identifier*) that are used to distinguish one object or person from others. These data can take many forms, and also a single object or person may have different identities associated. Authentication can be used to verify purported identities. An identity, which has been so verified, is called an authenticated identity

**masquerade:** pretence by a user to be a different user for any purpose

**Personal User Agent (PUA):** software, which performs actions, on the user's behalf, to facilitate the sending, management and reception of communications

**privacy:** right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. As a right, it is stricter than a requirement. The requirement in this case is that communications are secure enough as to preserve the privacy rights of the individuals

**receiver:** person receiving an incoming communication

**security:** term "security" is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.

**sender:** person making an outgoing communication

**smartcard:** smartcard is the size of credit card and has a microprocessor and storage capability embedded in it. It is capable of storing electronic data and programs that are protected by sophisticated security features

**trust:** generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function

**user:** person who uses a product or system (an end-user)

## 3.2 Abbreviations

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

| | |
|---|---|
| AI | Artificial Intelligence |
| CEC | Council of the European Community |
| CN | Common Name |
| CLI | Calling Line Identity |
| CLIR | Calling Line Identity Restriction |
| CNI | Called Name Identity |
| CNRP | Common Name Resolution Protocol |
| COLR | Connected Line Identity Restriction |
| DEG/HF | Draft ETSI Guide/Human Factors |
| DES | Draft ETSI Standard |
| DHCP | Dynamic Host Control Protocol |
| DNS | Distinguished Name Service |
| ES | ETSI Standard |
| ETSI | European Telecommunication Standards Institution |
| FCE | Future Computing Environments |
| GPS | Global Positioning Service |
| GSM | Global System for Mobile communications |
| GUI | Graphical User Interface |
| ID | Identification |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| ITU SG13 | International Telecommunications Union - Study Group 13 |
| MPA | Mobile People Architecture |
| PUA | Personal User Agent |
| PC | Personal Computer |
| PIN | Personal Identification Number |
| SIM | Special Information Module |
| SMS | Short Messaging Service |
| SMTP | Simple Mail Transfer Protocol |
| SSI | Service Specific Identifier |
| TIPHON | Telecommunication and Internet Protocol Harmonization over Networks |
| UCI | Universal Communications Identifier |
| UIFN | Universal International Freephone Number |
| UIPRN | Universal International Premium Rate Number |
| UISCN | Universal International Shared Cost Number |
| UMTS | Universal Mobile Telecommunications System |
| UPT | Universal Personal Telecommunications |

| | |
|---|---|
| URI | Universal Resource Identifiers |
| URL | Universal Resource Locator |
| URN | Universal Resource Names |
| WWW | World Wide Web |

# 4 Background

## 4.1 The rationale behind this guide

At present, users of communications systems are presented with a large and increasing number of methods of identifying parties with whom they wish to communicate. Contacting someone who possesses both a fixed and a mobile telephone often necessitates the remembering (or writing down) of two unrelated long telephone numbers. This same individual that is to be contacted may well have a different telephone and fax number if they are to be reached at work. They may also have more than one email address.

The present proliferation of pre-pay mobile telephones is resulting in a situation where no record exists of the person owning the telephone. There is currently no mechanism by which owners of pre-pay telephones can enable others to discover the identity of their telephones (e.g. no directories). The owners are thus entirely reliant on telling individuals what their telephone number is - which inevitably reduces the potential amount of incoming communication.

Solutions are available to enable users to control their different communication systems (e.g. supplementary services and mobility solutions) and to present a potentially simpler interface to the calling party. However all of these solutions differ in their method of operation and in solving one problem they may create others (e.g. setting diversion of a home telephone to the person's telephone at work will not be helpful to the caller specifically wishing to speak to somebody at the person's home). Also these solutions will only be used if the called party judges that their usefulness is worth the considerable effort needed to set them up.

People and organizations purchase terminals, network services or Internet services to enable them to create a more effective communications environment. Manufacturers and service providers develop new products and services to aid users in solving their communication problems and, in the process of selling these products, make profits. The existence of a more integrated method of identifying people and organizations could provide a clear focus and direction for manufacturers and service providers to follow in developing ranges of new products and services that work together to greatly enhance the users' experiences of communicating and of control over their communications needs.

There is a very clear need for an accurate and fundamental understanding of users' requirements both in setting-up and receiving communications. Whereas communications systems are developing at an increasingly rapid rate, many of the underlying communication needs of users (e.g. the need to talk to a specific individual, the need to talk to someone who occupies a specific work role, or the need to communicate with a person at a specific geographic location) have been the same since the earliest times. The availability of more sophisticated communications tools is changing peoples expectations and creating different communication needs, but these needs are still evolving slower than the rate of change of technology and they usually represent a modification of some more fundamental, but well established, communication needs.

These communication requirements need to be captured in an implementation-free form that enables them to be interpreted in specific ways in different communications systems in order to achieve a common integrated solution. This is the primary aim of the present document.

## 4.2 The structure of the guide

Annexes C and D examine the current and evolving communications environment. These identify some of the problems faced by, or that will be faced by, a user trying to use an environment that consists of a multitude of services and networks each with different identifiers.

The present document then delivers:

- A set of clearly stated implementation-free requirements (clauses 5, 6 and 7).

  The requirements are derived in a hierarchical way, considering, firstly, generic communications requirements, and then using these to develop a set of communication control requirements which, in turn, define the user requirements associated with an identifier.

  The set of identifier requirements thus obtained provide the criteria against which any proposed new identifier must be compared. In most cases this has to be a qualitative rather than quantitative comparison.

- An analysis of some commonly used personal identifiers in relation to the identifier requirements (clause 8).

- A number of identifier options that were rejected (clause 9).
  These are examined against the criteria defined above.

- A proposed solution (clause 10).
  This solution is explained and compared against the options that were rejected.
  The use of the preferred solution is illustrated by means of several scenarios (annex B).

- The implications of the proposed solution (clause 11).

- The benefits of the proposed solution and the migration issues in achieving it (clauses 12 and 13). Particular attention is given to the progressive implementation of the preferred solution.

- An analysis of what new standards and industry specifications are required (clause 14).

## 4.3 Potential users of the present document

This deliverable will be of value to Technical Bodies in ETSI as a set of requirements upon which their future standards can be based. Other standards bodies and commercial system developers will also be able to make use of this information.

The existence of proposed solutions in the area of user identification will provide a template and a roadmap that a number of future developments can realize over time, rather than provide a monolithic solution. From the outset of the implementation of the proposed solution, the increasing confusion associated with a multitude of IDs currently in use will be reversed towards a path of convergence to a simpler future environment for users.

# 5 Generic (high level) requirements

This clause examines the generic user requirements of a modern, ideal communications system. One objective of the present document is to identify ways in which this ideal can be approached. It should be noted that some of these requirements may wholly or in part conflict with other requirements. In developing any solutions based upon these requirements a judgement will have to be made as to which requirements cannot be fully met.

## 5.1 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 R1**

Users require a universal identifier and 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.

## 5.2 Reducing the impact of network boundaries

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 a sender to "experiment" until communication is established on one of the available networks than attempt to set up inter-network/inter-service communication.

For example, a sender first uses a fixed telephone to ring the receiver's fixed phone but gets a voice mailbox. The call is urgent so the sender 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 receiver'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 R2**

Users require seamless communication across networks and services.

## 5.3 Increasing the options available to the sender

At the present time, a sender has little control over outgoing communications other than by choice of terminal. In future the sender 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.

**User requirement No R3**

The sender of a communication requires the ability to indicate to the system particular requirements relating to the outgoing communication.

## 5.4 Increasing the options available to the receiver

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 receiver may also wish for the re-routing of communications to depend on the urgency of the call, who 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 R4**

The receiver requires the ability to control which communications are routed where, under what conditions and at what time.

## 5.5 Dealing with communications conflicts between sender and receiver

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

**User requirement No R5**

Users require that conflicts between the communication requirements of the sender and the receiver should be resolved, where possible, without their intervention.

## 5.6 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 R 6**

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.

## 5.7 Providing privacy

Users will have different requirements for privacy. Once most senders of communications can be identified by means of the universal identifier, a filtering process can be used exclude unwanted communications. Additionally it would 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 ex-directory function.

Both senders and receivers of communications may want the location from which they are communicating to be kept secret. Where communication occurs over fixed telephone networks, this may mean that suppression of the identity of the calling line or called line (CLI or COLI) will be needed in order to achieve this requirement.

**User requirement No R 7**

Users will require varying levels of privacy including location privacy.

## 5.8 User control of personal user agents

A very likely development in the future of communications is the use of network based software which undertake the role of a personal communications manger. This is sometimes referred to as a Personal User Agent (PUA). 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 R 8**

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 and that they should always have the ability to prevent the Personal User Agent from carrying out actions that they do not wish to happen.

## 5.9 Trust

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. Two primary circumstances where this is important are:

- when a communication is received the receiver needs to trust that the sender is that named in the presented identifier;
- when a sender initiates a communication the sender needs to trust that the party receiving the communication is the party named by the identifier that was used.

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 banking transactions, an additional method of verifying the identity and other characteristics of the party (such as their credit-worthiness) may be required. It is outside the scope of this work to determine whether the identifier used to identify the party when establishing the communication should also play a part in the further level of verification used in these higher risk transactions.

**User Requirement No R 9**

Users need to be able to trust that the party described by the identifier is the party with whom communication takes place.

# 6 Communication control requirements

In the current communications environment, each identifier is usually mapped to a single terminal or service. Although these existing identifiers will remain when universal identifiers are introduced, the use of such an identifier results in an environment in which a **single** universal identifier is associated with many terminals and services. In this environment, the user needs to influence the way in which terminals and services are mapped to the single universal identifier. The requirements in this clause reflect those functions that the user will require to perform in order to at least equal the flexibility provided when a range of different identifiers are available.

A common theme amongst all emerging architectures is the concept of a software entity or entities that manages the user's communications (see annex D). In particular, this entity would be aware of which terminals the user has access to, the probable location of the user, maintain communication histories, and take account of their communication needs. This software entity is referred to in the present document as a "Personal User Agent" or "PUA".

Several of the emerging architectures assume that the identifiers that are used (be they E.164 numbers or Internet URIs) will be personal identifiers rather than identifiers for terminals. This implies that the terminal may move with the user and that a user profile may be able to map the user to appropriate terminals. In cases where the identifiers no longer represent single terminals, the underlying systems must provide facilities that give users the same flexibility that they obtained from an understanding of which specific terminal was being contacted.

Current systems still provide the user with some information on the potential tariff of a communication based upon the identity of the number being contacted. Any future system is unlikely to be able to provide this potentially simple way of assessing communication costs and hence some alternative methods of providing tariff and cost information are likely to be provided.

Users are able to perform some call management based upon the characteristics of the number being called. Where future systems are not able to guarantee such a predictable relationship between the characteristics of the number and the nature of the terminal, some alternative means of allowing users to mange their calling strategies will need to be provided.

The priority assigned to a communication can sometimes be inferred from characteristics of the number that is calling or being called. Where this changes, future systems will need to provide a facility to determine and to set the priority associated with a communication.

All of the above implications will result in a number of additional user requirements needing to be defined that relate to the environment in which the personal identifiers operate.

## 6.1 User as communications manager

The facilities available from Personal User Agents/telecom servers will be subject to market forces. Some would provide a basic level of service; others could be more sophisticated with inbuilt AI to predict user needs etc. The following functions represent basic user requirements that should be met in all communication systems utilizing a Personal User Agent.

### 6.1.1 Providing communication configuration status

Users will soon have the opportunity to 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.

**User requirement No R 10**

Users require an indication of communication configuration status at any given time.

### 6.1.2 Editing the communication configuration

Given the complex configurations detailed in 6.1.1, the user will inevitably wish to make changes. These could entail over-riding the Personal User Agent for a specific communication, temporary changes to the configuration, (e.g. going away on business for two days) or a permanent amendment to the configuration (e.g. renting an extra fixed telephone line). The potential complexity of the configurations means that the user interface to the communication management program is critical.

**User requirement No R 11**

Users require the ability to easily edit their communication configuration.

### 6.1.3 Maintaining 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.

**User requirement No R 12**

Users may require a full communication history to be delivered.

### 6.1.4 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.

**User requirement No R 13**

Users may require their communications to be effectively managed dependant on their current location.

## 6.2 User as sender

### 6.2.1 Communication set-up requirements

#### 6.2.1.1 Access to personalized list of known user identifiers

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.

**User requirement No R 14**

Users may require an address book of user identifiers to be maintained. They may require this information to be duplicated in more than one physical or virtual location.

#### 6.2.1.2 Determining a personal identifier (if unknown) by means of a directory search process

The sender will require that all user identifiers are obtainable from a centralized database or many interconnected ones. The sender should be able to search based on a large range of attributes such as:

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

**User requirement No R 15**

Users require access to a directory (or directories) of user identifiers.

#### 6.2.1.3 Selecting communication medium and characteristics

Currently the medium for a communication is determined by the terminal used by the sender 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). Senders may also wish to specify the bandwidth or quality of a communication.

**User requirement No R 16**

The user may require the ability to select a communication medium as their first choice and specify attributes associated with that medium.

#### 6.2.1.4 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 e-mail voice note if a voice call can't be established and a voice-mail service doesn't exist).

**User requirement No R 17**

Users require that, when necessary, alternative options are tried in order to maximize the possibilities of them establishing communication (subject to any overriding requirements of the sender or receiver).

#### 6.2.1.5 Acknowledging social protocols

With current communications technologies, research by Anderson (see annex G) 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 "aware of" any prevailing social protocols such as the one mentioned.

**User requirement No R 18**

Users will require that relevant social protocols be reflected in the establishment of their communications.

#### 6.2.1.6 Providing cost information

Senders 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 a sender 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).

**User requirement No R 19**

Senders of communications may require that tariff information is made available to them so that they can predict the cost of a communication. Alternatively they may require that the accumulating or final cost be presented.

#### 6.2.1.7 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 receiver'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 receiver.

**User requirement No R 20**

Senders will require the ability to assign "urgency" to any communication.

### 6.2.2 Sender identification requirements

#### 6.2.2.1 Using the senders alphabet

The sender of a communication usually requires that their identity to be presented in the form in which it would normally be presented on paper. If the sender 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 receiver of the communication is able to display that alphabet. The sender still requires their identity be displayed in cases where the receiver of the communication is unable to display the senders alphabet.

**User requirement No R 21**

Senders require their identities to be presented using the alphabet in which their identity is normally presented on paper, where the receiver is capable of displaying that alphabet.

#### 6.2.2.2 Providing sender 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 sender of a communication even when the sender has chosen to be anonymous.

**User requirement No R 22**

Senders require the option of anonymity when establishing a communication.

#### 6.2.2.3 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.

**User requirement No R 23**

Users may require the option of assuming an alias.

### 6.2.3 Security requirements

#### 6.2.3.1 Validating receiver identity

In some cases, to ensure the security of their communications, the sender may require validation from the Personal User Agent that the receiver is who they claim to be. Contacting a bank, doctor or lawyer would be an example where this requirement would be important.

**User requirement No R 24**

Senders may require the ability to request the validation of the identity of the receiver.

## 6.3 User as Receiver

### 6.3.1 Call Receipt Requirements

#### 6.3.1.1 Identifying sender

The identity of the sender of a communication should be available to the receiver of that communication. If the identity of the sender is withheld for whatever reason (see Requirement **R 22**) then the receiver should be informed of this fact. Similarly if the sender is assuming an alias (see Requirement **R 23**) this should be indicated to the receiver. 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 a sender 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 sender of a communication even when the sender has chosen to be anonymous or is using an alias.

**User requirement No R 25**

A user requires the ability to unambiguously identify the sender of a communication or to be told that the sender is withholding their name or using an alias.

#### 6.3.1.2 Barring incoming communications from specified senders

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 e-mail 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 e-mail 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 ie 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.

**User requirement No R 26**

A user may require the ability to bar communications from selected senders.

#### 6.3.1.3 Managing incoming communications

The receiver will wish to set default conditions relating to the re-directing and filtering of incoming communications. The functionality associated with this communications management will vary greatly and be dependent on market forces. Examples of conditions that might be set are shown below.

*Sender a receiver may wish to filter communications dependent on the sender. Example: members of the immediate family could be allowed 24-hour real-time voice communication but business calls could be restricted.

*Date a receiver may wish to redirect communications on specific dates. Example: a receiver may wish to redirect all business communications at weekends to their email.

*Terminals available communications configurations will obviously be dependent on what terminals are available. Example: If a user purchases a new mobile then it is important that the system can be informed of its existence and how it fits into the re-directing/filtering strategy. This could involve complex configurations that will need to be interfaced in a user-friendly way.

*Priority assigned by sender a receiver may wish to route an incoming communication dependent on the priority assigned by a sender. Example: a user may wish to divert all incoming voice calls to a voice mailbox except those flagged as "urgent".

**User Requirement No R 27**

The receiver requires the ability to configure re-directing and filtering for incoming communications.

#### 6.3.1.4 Awareness of costs

Setting up a re-directing/filtering strategy may well have cost implications for the receiver. It is important that the receiver 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.

**User requirement No R 28**

Users may require the provision of costing information on different re-directing/filtering configurations.

### 6.3.2 Security Requirements

#### 6.3.2.1 Validating the sender's identity

In some cases, to ensure the security of their communications, the receiver may seek validation from the Personal User Agent that the sender is who they claim to be. This could be achieved by means of a PIN, smartcard, biometrics or other identification technology.

**User requirement No R 29**

Receivers may require the ability to request the validation of the identity of the sender.

# 7 Identifier requirements

Having defined the user requirements for an effective communications system, it is now possible to consider the requirements for an identifier which supports such a system.

Below are listed the requirements for an ideal user identifier. Inevitably some requirements are interdependent eg an increase in "robustness" (good) must mean an increase in "length" (bad). Inevitably then, the final choice of user identifier will be a compromise and the relative importance of each requirement therefore needs to be determined.

## 7.1 Uniqueness

Inputting a user's identifier as a communication address should identify that user amongst all other possible users. This is true global uniqueness. For the purposes of the present document, the user in this instance can be a person, an organization or a role within an organization. If the personal identifier identifies a person, then it must uniquely identify one person out of 6 Billion (i.e. every other person in the World). Where other entities are assigned identifiers of the same type as personal identifiers, the set of total identifiers might be even greater than the 6 Billion people in the world. This is an essential requirement.

**User Requirement No R 30**

Users require an identifier that uniquely identifies a person, organization or role within an organization.

## 7.2 Memorability

Modern terminals and network services with local storage of personal identifiers make memorability a less important attribute than it was but there are always going to be occasions where an identifier must be recalled and used from memory. One way to make a personal identifier memorable is to include some reference to the owner as in golden numbers (eg. 0800HERTZ) or email addresses (e.g. John.Smith@etsi.fr) or to use memorable digit runs (e.g. 123456). In the case of the telephony network, because of the limited combinations of letter and numbers this will always be a "premium" option for a relative few users. Email addresses still contain what are, to the sender, unmemorable alpha strings after the "@"which tend to negate the memorability of the name. Another way to increase memorability is to minimize the length of the identity. The memorability of any identifier can be enhanced when it is divided into small groups of characters, especially when these characters form some recognizable sequence or pattern. This process is referred to as "chunking".

**User Requirement No R 31**

Users require that the user identifier is easy to remember.

## 7.3 Length

The greater number of characters in a user identifier the longer the time to enter it on a terminal and the greater chance of an input keying error. Constraints of structure and inbuilt redundancy tend to increase the length of an identifier but as a general rule, identifiers should be as short as possible.

The negative effects of long strings can be improved by breaking them into more memorable blocks ("chunking"). Longer strings are, generally speaking, more difficult to remember and more prone to errors.

**User Requirement No R 32**

Users require the user identifier to be as short as possible.

## 7.4 Stability

There should be no requirement to change the user identifier every time the owner of the identifier changes an attribute (such as their address or their service provider). Some authorities conceive of a "Personal Identifier for life" where an identifier is only changed by a change of name e.g. marriage. Even where a change of name occurs, it is desirable that the original identifier will still correctly locate the intended recipient.

The concept of portability is a special case where a change of Service Provider does not require a change of user identifier. This is an essential requirement.

**User Requirement No R 33**

Users require that user identifiers are permanently allocated to a single person, role or organization.

## 7.5 Terminal independence

Communication terminals and their associated input devices are becoming more and more sophisticated but for the foreseeable future there will be a multitude of 12-button numeric keypads in existence i.e. basic telephones connected to very basic communications networks. Any future communication network(s) should not preclude use of such terminals even if they are only capable of achieving minimum levels of communication service.

**User Requirement No R 34**

Users require the ability to enter a user identifier on a basic 12-button numeric keypad connected to any type of network.

## 7.6 Searchability

Currently, access to identifiers varies greatly. In highly structured networks like the telephony network, finding a number if in possession of name & address details is relatively easy. In a less regulated environment such as the Internet, searching for an email address is difficult if not impossible. This is an unsatisfactory barrier to efficient communications which should be resolved in future systems. If the sender has sufficient information about the called party then, provided the receiver has allowed it, the identifier should be accessible by means of some sort of universal directory search.

**User Requirement No R 35**

Users require the ability to search for and find the personal identifier of "listed" users.

## 7.7 Robustness

Robustness can be defined as the ability of an identifier to cope with keying or memory errors. To be robust an identifier needs extra characters, which either provide error correction information, or duplicate/augment the primary characters. Robustness can be enhanced by thesaurus capabilities, locally or in the network, which can cope with alternative spellings in the case of identifiers that include names (e.g. Jon and John) or identifiers that include common words spelt differently in different countries (e.g. color and colour). Typically, the more robust a user identifier is, the more characters it will need.

**User Requirement No R 36**

Users require that when common misspelling and keying errors are made when entering a user identifier the systems it is used with should be able to cope.

## 7.8 Meaningfulness

The structure/content of user identifiers should be such that there is an indication as to whom the identifier belongs. Currently, Calling Line Identity (CLI) does not offer a meaningful identity for incoming telephony calls and its usefulness is reduced accordingly e.g. unless the terminal “recognizes" the incoming number from its limited directory, the terminal merely displays an E.164 number). Email addresses are often more meaningful (although not always) as there is the capability to have the name of the addressee as part of the identifier. Usually adding "meaningfulness" to an identity requires that the name of the owner of the identifier be included in some way in the identifier itself.

A meaningful user identifier is what someone receiving a communication usually requires, however someone sending a communication may wish to ensure that the receiver of a communication is not provided with meaningful information. In these circumstances the sending user would need to use an anonymous or alias identifier rather than their standard meaningful identifier.

**User Requirement No R 37**

Users receiving communications require user identifiers that contain the name of their owner - either a person, organization or a role.

## 7.9 Additional information

Requirement No R26 suggests that communications can be routed/filtered dependent on the sender (business or private) and Requirement No R25 requires that a receiver should know when an incoming communication is from an aliased or anonymous sender. It follows therefore that a user identifier should contain extra authentic and trustworthy information about the sender on which the receiver can base decisions on acceptance and/or routing.

**User Requirement No R 38**

Users may wish to be able to determine whether a communication is from a business or private source and whether the sender is remaining anonymous, communicating under an alias or using their correct name.

## 7.10 Authenticity

Users wish to be assured that when they receive a communication it comes from the person or entity that is described in the identifier (see Requirement No R9). For this to be the case, some trusted third-party needs to ensure that when an identifier is created the information it contains accurately represents the owner of the identifier. It is also necessary to ensure that once created, it is not possible for the identifier to be tampered with in order to change the information to something that does not accurately describe its owner.

**User Requirement No R 39**

Users require identifiers that contain information that they can be sure will always accurately describe the owner of the identifier.

# 8 User identifiers in common use

With the above attributes in mind, it is useful to look at three identifiers currently in common use and evaluate these against the defined identifier requirements (R30 to R39).

## 8.1 Name and address

Example:

John Smith,
123 Einstein Street,
Bentley,
Harrogate,
Yorkshire,
YO9 6AG,
United Kingdom

- Uniqueness (R30)

This is a unique identifier that identifies one particular person among all others. In some multi-occupancy accommodation the postal address may be non-unique where individual sub-units of accommodation are not numbered and persons with identical names occupy the accommodation.

- Memorability (R31)

As it consists in the most part of words and short alphanumeric strings it is relatively easy to memorize parts of the identifier but extremely difficult to accurately remember all of it.

- Length (R32)

The identifier consists of 87 alpha-numeric characters and spaces therefore entering the identifier is a relatively time consuming process.

- Stability (R33)

Any change of address effectively requires a change of personal identity; it is not therefore stable.

- Terminal independence (R34)

It is not possible to input such an identifier on a 12-button keypad except by lengthy keying codes.

- Searchability (R35)

Only the postcode is standardized and available on a centralized database. There is no standardized format for the rest of the identifier and the only databases of names and addresses (e.g. the UK Electoral Register) are not generally accessible. The massive redundancy (robustness) of the identifier will allow the database record to be found when incomplete information is entered.

- Robustness (R36)

There is a great deal of redundancy: in fact just a postcode, house number and name would be sufficient to identify the person. This means that the identifier is extremely robust so that misspellings and even omitted lines do not prevent communication (or delivery of a letter).

- Meaningfulness (R37)

This is as "meaningful" as an identifier can get. Nobody could be in any doubt as to whose identifier it is.

- Additional Information (R38)

A name and address may contain any amount of information in addition to that necessary to route the delivery of the mail. An indication of the urgency of the mail is a good example of the additional information that may be provided.

- Authenticity (R39)

Although there appears to be implicit information in a name and address about its source, any such information is unreliable. For instance the address given appears to be a private one but could in fact be a small business, or the name "John Smith" might be an alias.

- Other issues

Although this is a PERSONAL Identifier, communication can only be established if the person is currently located at the address included in the identifier. It is therefore very inflexible.

## 8.2 Telephone number

Example:

+441206643216

- Uniqueness (R30)

This is a unique identifier, but it only uniquely identifies a terminal and not a person or organization. Only in the case of a mobile telephone is it sometimes possible to indirectly identify a person.

- Memorability (R31)

The shortness of the telephone number increases the ability of users to memorize it. However, apart from golden numbers (such 123456), commonly used by commercial organizations, there are no aids to memorability apart from "chunking" which is usually implemented. Where groups of digits can be divided into chunks that are especially memorable because of some sequence or pattern, memorability can be further enhanced (e.g. 192 192 is likely to be more easily remembered than 19 21 92).

- Length (R32)

There is little redundancy, so given the constraints imposed by internationally standardized formatting, the identifier is as short as it can be. The hierarchical formatting allows abbreviation of the identifier dependent on location. (e.g. a sender communicating with a receiver in the same country need not input the digits associated with a country code thus shortening the number which needs to be memorized).

- Stability (R33)

Any change of terminal location (i.e. change of address) may require a new identifier (unless number portability is provided). If portability is not available, then the telephone number must also be changed if the Service Provider is changed.

- Terminal independence (R34)

The identifier consists only of digits and can therefore be input on any terminal.

- Searchability (R35)

Telephone numbers are standardized and highly structured. In each country operators maintain their own databases and these are accessible remotely. Theoretically, a sender can retrieve any public telephone number if they have appropriate search data. Searchability of corporate databases is usually restricted to employees of the same organization.

- Robustness (R36)

There is very little redundancy: a miskey would not normally be detectable by the system and would result in an incorrect connection.

- Meaningfulness (R37)

There is no meaningfulness in a telephone number except that the geographical origin of the communication can be determined in some circumstances. With increasing number portability this will be less and less the case.

No attribute of the number gives any obvious clue as to its owner apart from some "golden numbers" only used in a very limited number of cases.

- Additional information (R38)

There is no extra information in a telephone number that describes its originator although some sales publications insist that a "T" or "P" is typed after a number to indicate "trade" or "private". Terminals equipped with CLI will indicate when a number is being purposely withheld.

- Authenticity (R39)

Because telephone numbers are allocated by trusted telephone service providers in a structured manner the information they contain can be relied upon as being accurate. However, as the identifier contains no information about the identity of the owner, there is no actual authentic identification of the telephone number owner.

## 8.3 Email address (internet)

Example:

john.smith@myprovider.com

- Uniqueness (R30)

The hierarchical allocation of email addresses means that all email addresses are unique and identify a specific user, not a terminal.

- Memorability (R31)

Except for corporate email addresses, the character string after the "@" has little meaning for the caller and can therefore be difficult to remember.

As the number of people on a particular domain increase it may become impossible to have a unique "name" (e.g. john.smith will have to become john.r.smith or john.smith.2).

- Length (R32)

Email addresses are currently of a manageable length but it must be borne in mind that the number of email addresses in the world is increasing rapidly. It follows that producing a unique identifier may require longer addresses in the future.

- Stability (R33)

An email address does not offer stability as it is not portable. Any change of service provider requires a completely new personal identifier.

- Terminal independence (R34)

Email addresses require a full "qwerty" keyboard for input and cannot be input on 12-button keypads without the use of highly complex and time consuming key codes.

- Searchability (R35)

Identifier structure is typically dictated by the owner of the Domain in which the identifier resides. There is no universally adopted standard format or co-ordination. Although applications exist which purport to offer an email directory search service, they are extremely limited in their effectiveness.

- Robustness (R36)

There is little redundancy: a miskey would not be detectable by the system and would result in an incorrect communication.

- Meaningfulness (R37)

Some email addresses can be meaningful others less so. The current common format typically has the users first and family name (separated by a dot) in front of the "@". However with a quickly changing user population such as a university campus, users are often given meaningless number codes. In addition, with increasing email usage there will be more potential duplication of names and the resultant need to add numeric or other differentiators (e.g. john.smith24@myprovider.com.)

- Additional information (R38)

There is no reliable extra information in an email address. John.Smith could be an alias and the receiver does not know whether "myprovider" is a service provider or the company that John Smith works for.

- Authenticity (R39)

As private email account owners are usually free to choose the text they wish to precede the "@", there can be no guarantee that this information authentically represents the identity of the owner. It is likely that corporate entities will allocate authentic email addresses, but people receiving emails cannot always determine whether the email is from a company or from a private individual - so again they cannot be assured of its authenticity. Additional security mechanisms at the client or server end of email systems can provide reliable originator information that basic Internet email lacks

## 8.4 Implications arising from current identifiers

Requirement No R30, identifies "Uniqueness" as an essential attribute of a user identifier. Requirements Nos R31 "Memorability", R32 "Length", R33 "Stability", and R37 "Meaningfulness" all point to the desirability of a very simple identifier such as the person's or organizations name. However, virtually nobody's name will be unique in the context of total global communication.

Most existing identifiers either use a unique string of characters that bear no relationship to the user's name (e.g. an E.164 number), the user's name appended to the identity of another organization that may or may not have a known relationship to the person (e.g. albert.jones@hertz.com or mary.smith@cheapinternetnow.com), or the user's name with additional characters added to try to make the name globally unique (e.g. janet.w.jones@aa.com or john.smith123@compuserve.com). All of these types of identifiers employ strategies that create uniqueness, but each of them has deficiencies in one or more attributes of a good user identifier.

It can be seen that no current identifier scheme is without significant disadvantages that would preclude its use in a situation where communication could be across both the switched and IP networks. The proposed Universal Communications Identifier for converging networks must meet principal requirements R30, R33 and as many of the other requirements outlined in clause 7 as possible. It must minimize some of the disadvantages inherent in current addressing systems.

Table 1 summarizes the degree to which the attributes of current identifiers meet the requirements.

Table 1: Current identifiers

| User Requirements | Name and Address | Telephone Number | Email Address |
|---|---|---|---|
| Uniqueness (R30) | **** | ** | ***** |
| Memorability (R31) | ** | * | *** |
| Length (R32) | * | **** | *** |
| Stability (R33) | * | ** | *** |
| Terminal Independence (R34) | * | ***** | * |
| Searchability (R35) | * | ***** | * |
| Robustness (R36) | ***** | * | * |
| Meaningfulness (R37) | ***** | * | *** |
| Additional information (R38) | * | ** | * |
| Authenticity (R39) | * | * | ** |
| NOTE 1: ***** Meets requirement extremely well.<br>NOTE 2: * Does not meet requirement. | | | |

The telephone number is rated comparatively low on uniqueness as, although each number is always unique, it may not be uniquely associated with a single person and the association with any person is impossible to guess from looking at the number (see clause 5.9).

# 9 Rejected solutions

This clause describes a number of methods that have been proposed as solutions to the user identification issue. All of these solutions have been rejected as none of them meet sufficient of the User Requirements in clauses 5 to 7. Methods that meet the highest number of the User Requirements are described in most detail, whereas those that seriously fail to meet key User Requirements are not described so fully.

The proposals fall into two major groups:

- Methods for coping with multiple identifiers without using a new identifier;
- Methods that describe new Universal Communications Identifiers (UCIs).

Clauses 9.1 and 9.2 are two methods that do not rely on the creation of new identifiers, whereas the methods described in clauses 9.3 and 9.4 all use a new personal identifier.

Clause 9.5 summarizes the strengths and weaknesses of the various methods.

Email addresses are sometimes proposed as a possible solution. Email addresses are analysed in clause 8.3.

## 9.1 The directory-based multi-identifier solution

This solution assumes the existence of a universal directory service that contains the identifier (name or number) associated with each service/terminal combination that the user subscribes to/possesses.

### 9.1.1 Characteristics of the solution

This solution assumes that, when someone wishes to communicate with a new party, they are able to enter the details of that party into a universal directory enquiry service and the identifier needed to communicate using the chosen service is returned to the enquirer and, if required, the communication is set-up. When the identifier is returned to the enquirer, the enquirer will be able to store the identifier in his/her terminal for future use.

When a sender wishes to communicate with a recipient and searches for an appropriate identifier, in one variant of this solution, every one of the recipient's service/terminal identifiers are returned to the enquirer including the appropriate one for the immediate communication. If the sender's terminal is able to store multiple identifiers associated with a single person, then, in future, the sender would be able to communicate with the same recipient using any service to which the sender and recipient both subscribe without having to initiate a new search.

When only a single identifier is returned from an enquiry, senders have to perform a new enquiry each time they wish to communicate with the same recipient using a different service. In this option, the local storage of identifiers becomes somewhat more difficult to organize.

### 9.1.2 Meeting requirements

As this method does not have its own associated identifier, the assessment of how well the identifier requirements are met has to judged in relation to the many existing identifiers used in this method.

#### 9.1.2.1 Uniqueness (R 30)

Each identifier associated with a service/terminal is likely to be unique.

#### 9.1.2.2 Memorability (R31)

The memorability of many of the identifiers is poor (e.g. many telephone numbers) and the memorability of the complete set of identifiers needed to communicate with a person using any possible method of communication will obviously be worse.

#### 9.1.2.3 Length (R32)

Many of the individual identifiers are quite long. Again, the length of the complete set of identifiers is much longer. This may be an important issue if the user transcribes the individual identifiers from a business card to a local storage location (electronic or written).

#### 9.1.2.4 Stability (R33)

Many of the individual identifiers will change as users change their service providers and terminals (although number portability has reduced this instability). Another serious element of poor stability is where a user acquires additional terminals or services. The set of identifiers for someone's services/terminals that are stored in other peoples' terminals will not include any services/terminals that the user newly acquires. As time progresses, the relationship between stored identifiers and the actual services/terminals that a user currently possesses will become less and less correct.

#### 9.1.2.5 Terminal independence (R34)

The terminal independence of this solution will be good where stored identifiers match the service capabilities of the terminal in which they are stored. However, if the stored identifier is an email address and the terminal is a basic functionality telephone then the terminal independence requirement will not be well met. Where the caller frequently changes communication service and terminal when contacting the same person, then the danger that the stored identifiers are inappropriate for the required communication will become high unless all of the possible identifiers are stored in the terminal(s). The lack of an appropriate stored identifier will necessitate the caller needing to contact the directory enquiry service - which means that the poor terminal independence will not actually lead to an inability to communicate.

#### 9.1.2.6 Searchability (R 35)

As the whole method is based upon the presumption of effective directory search, it must be assumed that the searchability requirement is well met.

#### 9.1.2.7 Robustness (R 36)

The robustness of the identifiers in this method is as weak as the least robust identifier used.

#### 9.1.2.8 Meaningfulness (R 37)

The meaningfulness of the identifiers is as weak as the weakest identifier used. In particular, none of the telephone numbers involved in communicating will be particularly meaningful. A set of identifiers for different services/terminals is the core identification mechanism in this method. There is unlikely to be any meaningful relationships between many of the identifiers e.g. there will be no visible relationship between a telephone number and an email address for the same user.

#### 9.1.2.9 Additional Information (R 38)

The additional requirements capabilities will be the same as those of the individual identifiers.

#### 9.1.2.10 Authenticity (R 39)

The authenticity is likely to be quite weak as the authenticity of all identifiers in current use is weak.

## 9.2 The meta-search solution

This solution to the user identification issue involves the creation of no new identifiers. Instead it relies on a user being able to find any one of an intended receiver's service specific terminal identifiers if only one of these identifiers is known. If none of these specific terminal identifiers are known, then this solution assumes that the party wishing to communicate can obtain the service specific terminal identifier by means of a directory search in a directory associated with the required service.

### 9.2.1 Characteristics of the solution

The solution relies upon being able to search "existing" databases of service specific identifiers. It is difficult to see at present how this would work due to the lack of any comprehensive database of email addresses (existing solutions rely on people submitting their own email addresses to include, and they are little known or used). Also, all the other databases are unconnected and not all of them are globally electronically accessible.

Because a user's name is very unlikely to be globally unique, there is no way in which it is possible to ensure that any identifier obtained from a search is the one required. Because there is no agreed standard on any public database query interface, it is not possible to know what additional information, if any, could be supplied with the query to help to narrow the search.

One suggested means of obtaining the appropriate service specific identifier for a user is to do a search based upon a known service specific identifier for the same user but for a different service (e.g. to search for someone's email address if their home telephone number is known). The known service specific identifier can only be used in one of two ways:

1) The service specific identifier is used as a search term to look for resources (on the Internet) that include this identifier and one or more other service specific identifiers that belong to the same user. Examples of resources that might include this information are personal Web pages, author information in online published material, or a vCard [9] in a publicly searchable location. Currently, it is likely that searching for any of these resources on the internet will retrieve information on only a very tiny proportion of internet users, and an even smaller proportion of non-internet using telephony users. It is also the case that many of the resources that might be found may be out-of-date and therefore they will provide incorrect information.

   A quick study using Internet search engines was carried out to find the correct telephone number for people when their email address is known. For User A, using their main email address, led to a resource that contained no other identifiers, doing the same with a User B's email address produced nothing, and using the email address of User C also produced nothing. By using an internal directory (a method not available to 99,999 % of the population) it was possible to identify an alternative email address for User C, and using this produced a Web page that contained a telephone and fax number that could have been 6 months out-of-date.

2) A reverse-search is performed against the database of the organization that allocated the identifier in order to obtain the details of the owner. The details needed would have to be more than the name, as this is unlikely to be unique and is likely to be known to the user performing the search. If sufficient information can be obtained to uniquely identify the owner of the service specific identifier then this information could be used to search other databases in order to obtain the other required service specific identifier(s). This approach has two major limitations:

   - obtaining sufficient information is likely to be considered a major invasion of privacy by the owner of the identifier;

   - other databases may not contain the same information fields as that of the database initially searched and the information in matching fields may also conflict in some cases. This would cause searches to fail.

## 9.2.2 Meeting requirements

As this method does not have its own associated identifier, the assessment of how well the identifier requirements are met has to judged in relation to the many existing identifiers used in this method.

### 9.2.2.1 Uniqueness (R 30)

Each identifier currently associated with a service/terminal is likely to be unique. However, if an identifier has been retrieved from an outdated source of information, it may be allocated to another individual to the one expected (this may frequently apply to telephone numbers in short-term rented accommodation).

### 9.2.2.2 Memorability (R31)

The memorability of many of the identifiers is poor (e.g. many telephone numbers). As this solution proposes that any identifier may be used to access a user irrespective of the service being used, the overall rating for memorability will depend on which service specific identifier is memorized.

### 9.2.2.3 Length (R32)

Many of the individual identifiers are quite long. As with memorability, the rating for length will depend on the service specific identifier that is used.

### 9.2.2.4 Stability (R33)

Whenever an identifier is recalled from some personally held list of identifiers and is used to try to initiate a communication, there is a risk that the identifier is no longer valid. The longer time that elapses from the local storage of the identifier to its usage, the greater that risk becomes. If the identifier is now unallocated, it is suggested that a current identifier could be obtained and used by means of a reverse database lookup in a database of superseded identifiers. This method is fraught with privacy issues and is currently not achievable. If the identifier had been re-allocated, as currently happens, then the communication would have been set-up to the wrong party. Taking these limitations into account, this proposal must be given a low rating on "stability".

### 9.2.2.5 Terminal independence (R34)

This proposal does not adequately address the terminal independence issue. If the known identifier is the user's email address, this cannot be directly input from a conventional 12-key telephone. Although voice-based interfaces could be used to enable the email address to be dictated from a telephone, this is a very cumbersome and inadequate substitute for genuine terminal independence.

### 9.2.2.6 Searchability (R 35)

The proposal relies very heavily on the ability to search for identifiers. As discussed in 9.2.1, it is not felt that the proposed methods of search will be sufficiently effective in practice.

### 9.2.2.7 Robustness (R 36)

The robustness of the identifiers in this method is as weak as the least robust identifier used.

#### 9.2.2.8 Meaningfulness (R 37)

The meaningfulness of the identifiers is as weak as the weakest identifier used. In particular, none of the telephone numbers involved in communicating will be particularly meaningful.

#### 9.2.2.9 Additional Information (R 38)

The additional requirements capabilities will be the same as those of the individual identifiers.

#### 9.2.2.10 Authenticity (R 39)

The authenticity is likely to be quite weak as the authenticity of all identifiers in current use is weak.

## 9.3 Internet "Common Name" (CN)

### 9.3.1 Characteristics of the identifier

The IETF "Common Name" (CN) (see clause D.4.3) has been proposed as a word or phrase, without imposed syntactic structure, that may be associated with a resource. Common Names are expected to be used primarily by humans (as opposed to machine agents). The IETF documents (see "Context and Goals for Common Name Resolution", annex G) indicate that they lack syntactic structure; there is no requirement of uniqueness or persistence of the association between a common name and a resource.

### 9.3.2 Usage of the identifier

A likely usage scenario is users would input a CN into the free-text input field of an Internet browser in the same way in which they would input a URL. The "Common Name Resolution Protocol (CNRP)" would be used to try to resolve a URL that pointed to a resource to which the CN is referring and then the user would be connected to that resource (e.g. Web page).

### 9.3.3 Meeting requirements

#### 9.3.3.1 Uniqueness (R 30)

The Internet Draft (see "Context and Goals for Common Name Resolution", annex G) explicitly states that there is no requirement for uniqueness.

#### 9.3.3.2 Memorability (R31)

As there are no syntactic constraints and no constraints on uniqueness, it is possible to make the CN as meaningful as possible - indeed this is its primary purpose for existence.

#### 9.3.3.3 Length (R32)

As there is no syntactic constraints and no constraints on uniqueness, it is possible to make the CN as short as possible whilst retaining meaningfulness.

#### 9.3.3.4 Stability (R33)

The Internet Draft (see annex G) explicitly states that there is no requirement for persistence of the association between a common name and a resource.

#### 9.3.3.5 Terminal independence (R34)

The CN cannot be directly entered on a 12-button keypad to a basic telephone network. The CN is clearly intended as an identifier that must be entered into an Internet connected terminal that can directly utilize the CNRP protocol.

#### 9.3.3.6 Searchability (R 35)

Given that the Common Name is likely to be one of the primary search terms used it is unlikely that people would ever explicitly search for Common Names. However it is likely that the Common Name would be one of the items returned by a search-engine in a general search related for the resource that is referenced by the CN.

#### 9.3.3.7 Robustness (R 36)

As the CN is, by definition, a common name, it is subject to all the mis-spellings that can frequently occur when people believe that they know how a name is spelt but where their idea of the spelling is incorrect.

#### 9.3.3.8 Meaningfulness (R 37)

Users receiving communications require user identifiers that contain the name of their owner - either a person, organization or a role.

#### 9.3.3.9 Additional Information (R 38)

Users wish to be able to determine whether a communication is from a business or private source and whether the sender is remaining anonymous, communicating under an alias or using their correct name.

#### 9.3.3.10 Authenticity (R 39)

The authenticity of a CN is dependent on the, as yet undefined, mechanisms for creating CNs. If this is a well controlled activity that seeks to obtain proof that the person or organization requesting the CN is entitled to use that name, then authenticity will be good. Without such a mechanism, authenticity cannot be assumed.

## 9.4 Internet URN

### 9.4.1 Characteristics of the identifier

URNs are defined in an Internet Request for Comment [8]. Their functional capabilities are described as:

- Global scope - "A URN is a name with global scope which does not imply a location. It has the same meaning everywhere";
- Global uniqueness - "The same URN will never be assigned to two different resources";
- Persistence - "It is intended that the lifetime of a URN be permanent";
- Scalability - "URNs can be assigned to any resource that might conceivably be available on the network, for hundreds of years";
- Legacy support - "The scheme must permit the support of existing legacy naming systems …";
- Extensibility - "Any scheme for URNs must permit future extensions to the scheme";
- Independence - "It is solely the responsibility of a name issuing authority to determine the conditions under which it will issue a name";
- Resolution - "A URN will not impede resolution (translation into a URL, q.v.)".

### 9.4.2 Usage of the identifier

URNs may be input by human users or they maybe generated by software applications controlled by user. URNs will be read by software and translated into other identifiers for use. One possible use of URNs is as user identifiers that can be used as part of a communications environment.

### 9.4.3 Meeting requirements

#### 9.4.3.1 Uniqueness (R 30)

The Internet Request for Comment that defines URNs [8] explicitly states that they must have "Global uniqueness".

#### 9.4.3.2 Memorability (R31)

As URNs must be unique for all people and roles on a global scale, they are likely to be long enough and/or complex enough to be less memorable than a simple personal name.

#### 9.4.3.3 Length (R32)

As the only constraint on URNs is that they are unique, their length can be made the minimum necessary to achieve uniqueness.

#### 9.4.3.4 Stability (R33)

The Internet Request for Comment that defines URNs [8] explicitly states that they must have Persistent and hence must satisfy the "Stability" requirement.

#### 9.4.3.5 Terminal independence (R34)

As all proposed definitions of URN syntax assume that the leading characters will be "urn:", they clearly cannot be directly entered on a 12-button keypad to a basic telephone network. The URN is clearly intended as an identifier that must be entered into an Internet connected terminal, either directly or via some application support. However, it is possible to imagine that, if the actual URN itself were numeric, this header could be added at the interface between the telephony local access point and the Internet.

#### 9.4.3.6 Searchability (R 35)

As URNs are unique and are assigned by a naming authority, it must be possible to search for them using the information provided at the time of registration. For this searching to be meaningful, sufficient information must have been provided at the time of registration and a search mechanism must have been provided. Neither of these pre-conditions is listed as requirements of a URN system, but also, neither of these possibilities is excluded.

#### 9.4.3.7 Robustness (R 36)

The robustness of the URN is dependant on the syntax of the URN and on any inherent parity check characters that may be included in the identifier when it is allocated. It is assumed that URNs are likely to be allocated in a manner that does not provide enhanced robustness.

#### 9.4.3.8 Meaningfulness (R 37)

One way of adding meaningful information to a URN is by concatenating meaningful information on the owner (such as their name) with other information that will guarantee its uniqueness However, such an approach cannot be used as a URN is required to be both unique and persistent, and the information on the owner cannot be guaranteed to be persistent over all time (e.g. the surname of a woman may change when they marry). Hence, it is not possible to achieve uniqueness, persistence and meaningfulness simultaneously.

#### 9.4.3.9 Additional Information (R 38)

No mechanisms for conveying additional information are suggested in IETF documents that describe URNs.

### 9.4.3.10 Authenticity (R 39)

As URNs are allocated by a naming authority, their authenticity can be assured at the time of creation. For people other than the owner of the URN, the authenticity can only be guaranteed where trust relationships exist between all parties (the URN owner, the URN reader and the URN issuing authority).

## 9.5 Comparison of personal identifier solutions

Table 2 shows a summary of how the identifiers in the various proposed identification solutions meet the User Requirements for user identifiers described in the present document.

**Table 2: Comparison of all proposed personal identifiers**

| User Requirements | Directory-based Multi-identifier | Meta-search | Internet Common Name (CN) | Internet URN |
|---|---|---|---|---|
| Uniqueness (R30) | ***** | *** | * | ***** |
| Memorability (R31) | * | ** | ***** | *** |
| Length (R32) | ** | *** | ***** | ***** |
| Stability (R33) | * | * | * | ***** |
| Terminal Independence (R34) | *** | * | * | * or ***** see clause 9.4.3.5 |
| Searchability (R35) | ***** | ** | *** | *** |
| Robustness (R36) | ** | ** | ** | ** |
| Meaningfulness (R37) | ** | ** | ***** | ** |
| Additional information (R38) | * | * | * | * |
| Authenticity (R39) | * | * | * or ***** see clause 9.3.3.10 | ***** |
| NOTE 1: ***** Meets requirement extremely well.<br>NOTE 2: * Does not meet requirement. | | | | |

As can be seen from table 2, it is not possible to rate the effectiveness of the user identifier in the "The directory-based multi-identifier solution" and "The meta-search solution" solutions (clauses 9.1 and 9.2) as no new user identifiers are proposed. Instead, with these solutions, users have to deal with any or all of the current and future service specific identifiers associated with the parties they wish to contact.

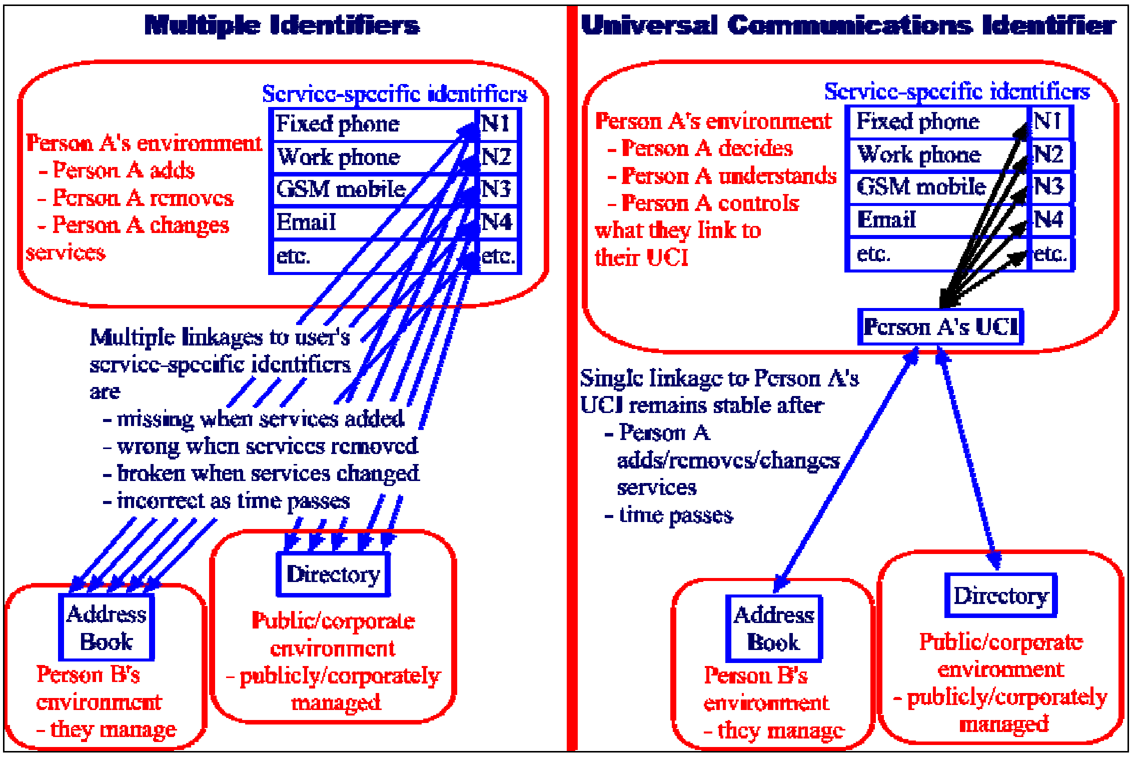

Multiple Identifiers
Service-specific identifiers
Fixed phone
Work phone
GSM mobile
Email
etc.
N1
N2
N3
N4
etc.
Person A's environment
- Person A adds
- Person A removes
- Person A changes
services
Multiple linkages to user's service-specific identifiers are
- missing when services added
- wrong when services removed
- broken when services changed
- incorrect as time passes
Address Book
Person B's environment
- they manage
Directory
Public/corporate environment
- publicly/corporately managed
Universal Communications Identifier
Service-specific identifiers
Person A's environment
- Person A decides
- Person A understands
- Person A controls
what they link to their UCI
Fixed phone
Work phone
GSM mobile
Email
etc.
N1
N2
N3
N4
etc.
Person A's UCI
Single linkage to Person A's UCI remains stable after
- Person A adds/removes/changes services
- time passes
Address Book
Person B's environment
- they manage
Directory
Public/corporate environment
- publicly/corporately managed

**Figure 1: A comparison of multiple- identifier and UCI approaches**

One of the primary flaws in both multi-identifier approaches is the inevitable disconnection that will occur between the set of identifiers relating to PersonA stored in a PersonB's address books (or in a unified public directory system) and the set of services and service identifiers that are actually possessed by PersonA. In the multi-identifier scenario, any changes made to PersonA's communications environment cannot be reflected in the address books and directories that are managed by others. The complexities and disconnections inherent in multi-identifier solutions are shown in the left-hand side of figure 1.

In contrast, the right-hand side of figure 1 shows how PersonA can always ensure that all elements of his/her communication environment will be linked to his/her Universal Communications Identifier (UCI). In most cases when a change to PersonA's environment is made, the provider of the new service can ensure that a link is automatically made to PersonA's UCI. Figure 1 illustrates how any solution that uses a Universal Communications Identifier (UCI) brings the potential to bring a high degree of stability in the accuracy of the information stored in addresses books and directories.

In summary, both the proposals that do not require a new identifier to be used suffer significantly in the way in which they fail to adequately address the "stability" issue. Also, both options expose to users all of the weaknesses associated with the individual service specific identifiers (e.g. long number length, lack of meaningfulness, poor memorability).

A further serious concern with the "Meta-search proposal" is the assumption that known identifiers may be used as a key to locating other identifiers for the same user. This approach is based upon a presumption that a lack of stability of identifiers, due to them being no longer used, can be worked around in the searching mechanisms. It seems likely that one of the few ways in which this could be achieved is by the privacy threatening method of reverse database lookup. This approach also ignores the problems that might occur if an identifier is re-allocated instead of becoming redundant. Finally, this approach does not appear to address terminal independence issues.

Moving on to single identifier solutions, the identifier proposed in the "Internet Common Name (CN)" proposal (clause 9.3) can be dismissed as a serious candidate for a Universal Communications Identifier on one ground alone - it is not expected to be unique. Although the CN has a useful role to play in the general field of identifying resources, this lack of uniqueness and several other key characteristics such as stability and terminal independence make it completely unsuitable in this role.

The "Internet URN" that is described in clause 9.4 has many excellent characteristics for a Universal Communications Identifier including uniqueness and stability. Because its intended use presupposes an initial header of "urn:", it cannot be directly or easily entered from a 12-button telephone and, hence, cannot fully meet the "Terminal Independence" requirement. However, it is possible to imagine that, if the actual URN itself were numeric, this header could be added at the interface between the telephony local access point and the Internet. The final difficulty that the URN has is that, irrespective of the content and format of the URN string, it cannot overcome the conflict that exists between uniqueness, meaningfulness and stability that is discussed in clause 8.4.

# 10 The proposed solution

The arguments in clause 8.4 show that it appears to be impossible to ensure uniqueness and also satisfy the criteria of memorability, length, stability and meaningfulness in a user identifier that comprises a single string of characters. As a result of this fact, the proposed solution is a user identifier as shown below.

This consists of:

1) An alphabetic label that is the name by which the user usually wishes to be known. This is the most user-friendly label possible in that it is the label that the user naturally chooses to call themselves. Although it is undoubtedly user-friendly it is unlikely to be unique. It may, however, be unique in a certain limited context as explained later.

   Where the user normally writes their name using a non Latin alphabet, two variants of the label would be required to meet User Requirement No R21. The first variant of the label would be in the alphabet used by the user when writing their name. The second variant of the label would be in the Latin alphabet, with names written in the manner most appropriate when that alphabet is used.

2) A numeric string that is globally unique. To be globally unique, this number must be fairly long and so it is not likely to be very user-friendly. This numeric string is the address of the Personal User Agent belonging to the person or organization to which the UCI is allocated.

3) An additional part of the label which imparts extra information in the form of flags. These flags could indicate whether the communication is from a corporate source or a private one, and whether the visible part of the label is a real name or an alias (User Requirement No R39).

As the usage scenarios discussed in annex B illustrate, it is expected that in most circumstances users will not actually need to explicitly input the numeric string element of the user identifier into the system. They are likely to either search for a user and have the communication system automatically establish the communication session or to recall the user identifier from a list of stored Universal Communications Identifiers. Dependant on the final implementation of a universal identifier system, the UCIs could be stored in terminals, on Smartcards, printed or coded onto business cards, stored in a network, etc. In the case where the UCI is stored, the user sees the alphabetic label and the communication system uses the numeric string and additional information.

## 10.1 Characteristics of the identifier

### 10.1.1 Characteristics of the alphabetic label

The alphabetic label is designed to carry information that describes the owner of the Universal Communications Identifier in the way in which they wish to be described. There are at least 2 possible variants of this label for use by private individuals:

1) A name that accurately indicates the real identity of the owner of the Universal Communications Identifier. This is a Universal Communications Identifier that can be trusted by third parties as being accurate (Requirement No. R39).

   In order to ensure that the alphabetic label is unambiguous and also that it can be stored in address book storage the Forename and Surname need to be in a predictable order. This is to ensure that the user receiving the UCI can tell whether "Peter Christian" is someone with the Forename "Peter" and the Surname "Christian" or the reverse.

   The suggested option for at least European and American labels is to have Forename followed by Surname. Where the national or regional convention differs from Forename followed by Surname, the national or regional convention would be followed in the ordering of the label. This restriction need only apply for the first option above where a true and accurate label is being used. The presentation order used could be indicated in the additional information field.

2) A name that represents an alias by which the owner of the Universal Communications Identifier wishes to be known. Where such an alias is used it should be possible for people receiving communications associated with this Universal Communications Identifier to know that the identifier does not accurately represent the true identity of the owner. The case of a completely anonymous communication, where the alphabetic label is blank, is a special case of the alias variant and can be treated similarly (Requirements Nos. R22 and R23).

For corporate Universal Communications Identifiers, the label would be a name that includes the identity of the organization that owns the Universal Communications Identifier. Where the Universal Communications Identifier represents a role within an organization, it is the responsibility of the organization to determine the detailed content of the label, but an element of that label must be an accurate identity for the organization (Requirements No R25, R26, R27, R38 and R39).

Where the user writes the content of the label in an alphabet other than the Latin alphabet, two versions of the label would be required. The first version would present the information in the label in the manner in which it would normally be presented in the user's alphabet. As a fallback option, the second version would present the information in the manner in which the user would normally present it when only the Latin alphabet can be used. Which version of the label is presented would be subject to negotiation between PUAs.

### 10.1.2 Characteristics of the numeric string

#### 10.1.2.1 Basic Format

Requirement No R34 states that a person should be able to enter a user identifier using the most basic terminal. This Requirement and Requirement No R6 on backward compatibility imply that the terminal could be a terminal on any network, including those that have not yet fully adopted the new Universal Communications Identifier handling system.

In a scenario where a whole country or network operator does not support the proposed user identification handling scheme, a number of compatibility issues point very strongly to the numeric element of the Universal Communications Identifier being an E.164 number. Two sub-options of this scenario need to be considered:

1) Directly dialling the Numeric String of the UCI

   In this case the numeric string to be dialled must not be part of the national numbering plan of the non-participating country as the telephone system would then try to (unsuccessfully) process the UCI number as a national telephone number. Given the variability of the structuring of national numbering plans and given that a range of numbers large enough to handle every person, role, organization and location in the world must be found, it would be impossible to guarantee that the numeric strings were not part of an existing national numbering plan.

The implication of this finding is that the numeric string would need to be treated as outside the national numbering plan in the non-participating country and that it needs to be uniquely and globally managed. This further implies that, in the non-participating country, the numeric string must be dialled in the same way as an E.164 number is dialled in that country – with the first part of the numeric string acting as a country code and routing the communication to a participating country where the numeric string can be resolved by the user identification handling system. In other words the numeric string must be an E.164 number.

2) Indirectly dialling the Numeric String of the UCI.

   An option that does not predetermine the format of the numeric string in any way is indirect dialling. In this case, the caller would have to dial some initial digits that provided access to a system that could accept and forward the digits from the numeric string and possibly participate in some more limited way in the further handling of the proposed user identifiers (e.g. some more limited negotiation capability).

   Each country would be free to allocate digits for access to this UCI forwarding service and they could be free to choose the degree of sophistication of that service.

The first of these two options places no demands on countries that choose not to participate in the UCI handling scheme. The second option implies that all countries that choose not to participate in the UCI handling scheme must put into place services that can handle the new UCIs if their citizens, or visitors to their country, are to be allowed to communicate with the rest of the world. The second option seems unlikely to be accepted by the telecommunications/internet world.

#### 10.1.2.2 Robustness

When the numeric part of the identifier is standardized, the option will be available to include check sum digits in the string. Use of check sum digits immediately flags up any error in keying to the system and the sender can be asked to check and re-key. But as with so many other issues there is a trade off between the robustness created by the check digits (R36) and the length (R32) and the memorability (R31).

It is even possible to add sufficient digits to the number string to enable detection AND correction of a single error but the resulting length of such a number string would probably be unacceptable.

#### 10.1.2.3 Authentication source

Independent of the method of number allocation, it will be necessary to be able to identify the authentication authority from the number string. This will be an important requirement because a request for verification of sender or receiver will require reference to the relevant authority by the PUA. This information must therefore be available within the Identifier.

If the numbers are allocated in blocks to each authority in the same way as an E164 number, then this information will be embedded in the number automatically. If numbers are allocated on a more ad-hoc basis then there may need to be a special field within the number string identifying the authentication authority.

### 10.1.3 Characteristics of the additional information field

To satisfy requirements Nos R26 and R27, an additional field which can be used by the receiver to determine whether a communication is from an authentic business, an authentic private individual or an alias. It should be noted that it is expected that a communication using an alias will not be identified as being either a business or an individual. In the future other requirements may become apparent necessitating the inclusion of other data in this field.

The field itself would consist of "flags" and would not be directly visible to the user. These flags could be interpreted by the receiver's PUA and presented accordingly e.g. as a warning window on a PC, simple text on a mobile telephone display or as a voice message on a basic fixed telephone. The flags could also be used by the PUA in implementing the receiver's routing/filtering configuration e.g. the diverting of all business calls to a mailbox.

## 10.2 Usage of the Universal Communications Identifier

In the next four clauses the ways in which Universal Communications Identifiers are used for establishing a communication, receiving a communication, capturing a UCI and managing the communication environment is described.

### 10.2.1 Establishing a communication

There are three basic scenarios that describe the ways in which the Universal Communications Identifier might be used, although many other variants could be conceived. These scenarios are:

1) Direct entry of the UCI

   This is expected to be the least common and least well supported method of entry. It is, however, the one most similar to that used in a high proportion of current communications - both by telephone or email.

   In this scenario the user establishing the communication would need to enter the numeric part of the UCI directly into the terminal. Where the terminal only has a numeric keypad and no other facilities such as number memories, this might be the only method available.

2) Recalling the UCI from a Memory Store

   This method is very similar to the way in which users of mobile telephones and emails frequently manage their communications. The UCI of those parties with whom a person most frequently communicates would be stored in a personal store of UCIs (in the person's terminal and/or in the network). When the user wishes to communicate with one of the parties whose UCI is held in store, they would access the UCI by selecting one Alphabetic Label from the set of all the Alphabetic Labels. This could be done by selecting the Alphabetic Label from a list presented on the screen of the Terminal or by speaking or typing all or part of the Alphabetic Label into their terminal (the precise method of accessing stored UCIs would be a matter for terminal manufacturers).

   In this method, the sender would only need to use the Alphabetic Labels with which they should be very familiar and not the Numeric String which they might not know.

3) Searching for the UCI

   An essential component of the new UCI system is a means to perform a global search for any UCI. A potentially wide range of data would be stored for each UCI owner, and this could be matched against in any search. Examples of the data are the party's address, employer or date and place of birth. The owner would be given the right to determine which elements of the information could be searched against and which elements could also be released to other parties. The default might be that all information could be searched against but that only the UCI could be released.

   After a successful search, the default action would be to return the UCI to the user conducting the search and to offer to establish communication. However, a further protection of privacy could be to only offer to establish the connection and not to release the UCI to the user performing the search.

### 10.2.2 Managing incoming communications

The inclusion of the UCI of the sender will enable the receiver, or the receiver's Personal User Agent, to make decisions about how to deal with incoming communications.

1) Filtering/routing by the Personal User Agent

The receiver's Personal User Agent will have communication rules to enable decisions about how to route and/or filter the incoming communication. These rules will depend on a range of factors including time of day, priority etc. but, almost certainly, information contained in the UCI will also be important. For instance, the Personal User Agent may well have a list of UCIs which are allowed real-time voice access any time of day (close family perhaps). Other information in the UCI such as whether the sender is private/commercial or has provided their real name/alias/anonymous may well dictate how the communication is dealt with.

2) Information presented to the receiver

The fact that the receiver's Personal User Agent knows the identity of the sender means that the sender's name can be displayed on any terminal with an appropriate display capability. This will be far more powerful and meaningful than the CLI service currently available which normally only displays a number. Local decisions, such as accepting or not accepting the communication, can then be made by the receiver.

3) Editing the UCI based routing/filtering rules

The use of the sender's UCI (and other criteria) by the recipient's Personal User Agent to make decisions with respect to the routing and filtering of incoming communications has been described above.

The rules by which this is done will almost certainly be complex and designing the user interface to the incoming communications management part of the PUA will be a challenging task. Some rules will be dependent on the sender's UCI, others may not.

Key to the editing of routing/filtering rules dependent on the senders UCIs will be the receiver's centrally stored address book where all regularly used UCIs will be listed. Storing the address book centrally ensures that its content can be retrieved both by the user and by the PUA irrespective of which terminal is being operated by the user. The receiver will be able to create special groups and distribution lists (close family, social club members etc) within the address book which will facilitate the editing of the routing/filtering rules.

### 10.2.3 UCI Capture

Where, after a search, the UCI is released to the user performing the search, the possibility would exist for them to capture that UCI in their local store. Also the UCI that would be delivered when an incoming communication is received could also be captured. Dependant on the final implementation of a Universal Communications Identifier system, the UCIs could be stored in terminals, on Smartcards, printed or coded onto business cards, stored in a network, etc.

Once the form of the UCI has become standardized, it would be very likely that manufacturers of terminal equipment would produce terminals in which capture of UCIs would be a one-button (one spoken command) action. When the UCI is stored both a number and label would be stored and the label would be the "user friendly" access mechanism for retrieval of the UCI.

This UCI capture mechanism would be an enhancement of the facility that currently exists in many terminals whereby the CLI of the calling party can be stored in the users terminal but where the terminal owner then has to enter their own label to identify the stored number. This usage is currently common both in the voice telephony and email environments.

### 10.2.4 Graphical illustration of basic communication using a directory service

The diagrams below are purely illustrative and nothing should be inferred with regard to network architectures or services. They show just two of many ways in which a UCI could be used to assist in the setting up of communications in the future.

In figures 2 to 4 John is trying to communicate with Wendy. He does not know her UCI.

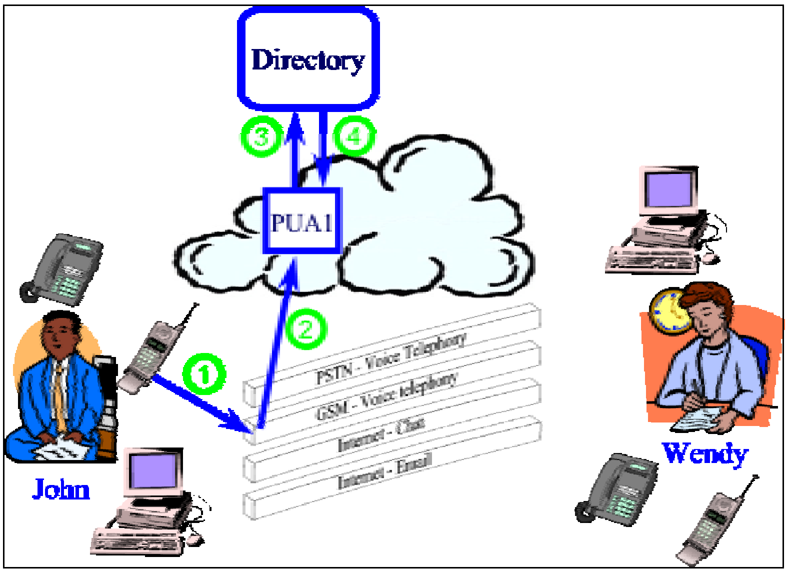


**Figure 2: Searching for an unknown UCI**

① John scrolls the address book in his mobile and locates "new contact" in the display. He then presses the "send" button implying that he wants to make a call but does not know the Universal Communications Identifier of the intended receiver.

② The GSM Network connects John to his PUA.

③ The PUA is aware that the call from John is on a mobile with no alpha keyboard so accesses a speech recognition based directory service.

④ John gives the directory service Wendy's name and other details that identify her UCI. John's PUA puts Wendy's UCI in his address book for future usage (this description is slightly simplified - a more detailed description of how information might be returned from a directory service is given in clause 11.3).

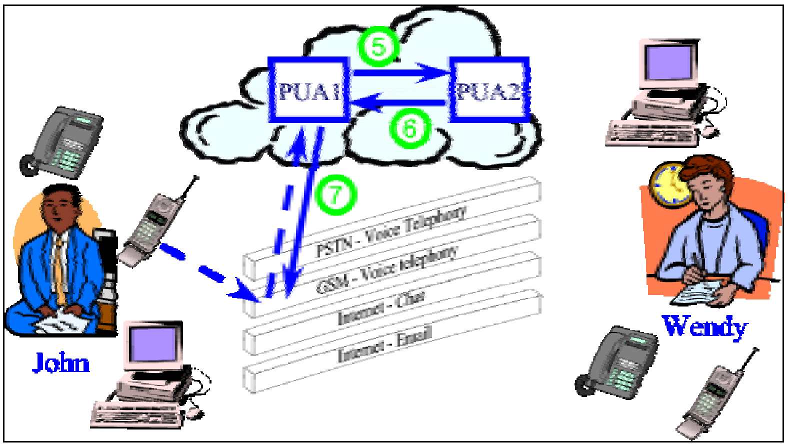


**Figure 3: Negotiating and retrieving the service specific terminal identity**

⑤ John's PUA now communicates with Wendy's PUA via the IP Network offering a voice communication via GSM.

⑥ Wendy's PUA tells John's PUA that her mobile is currently switched off and unavailable. It suggests contact via the PSTN and supplies the PSTN terminal address.

⑦ John's PUA now returns Wendy's PSTN number to enable the network to set-up the call.

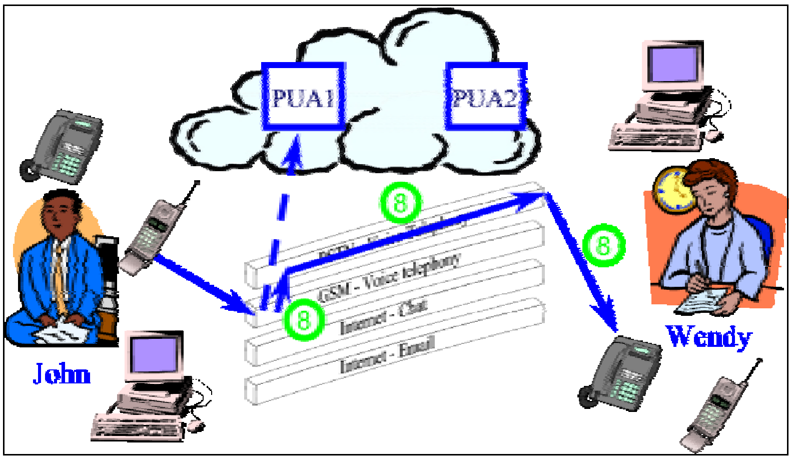


**Figure 4: Establishing the communication path**

⑧ Communication is established.

### 10.2.5 Graphical illustration of communication across networks

The use of UCIs is further illustrated by the next three figures. Again, John wants to speak to Wendy. Now, he has her UCI in his address book but in this case no speech path is available between sender and receiver.

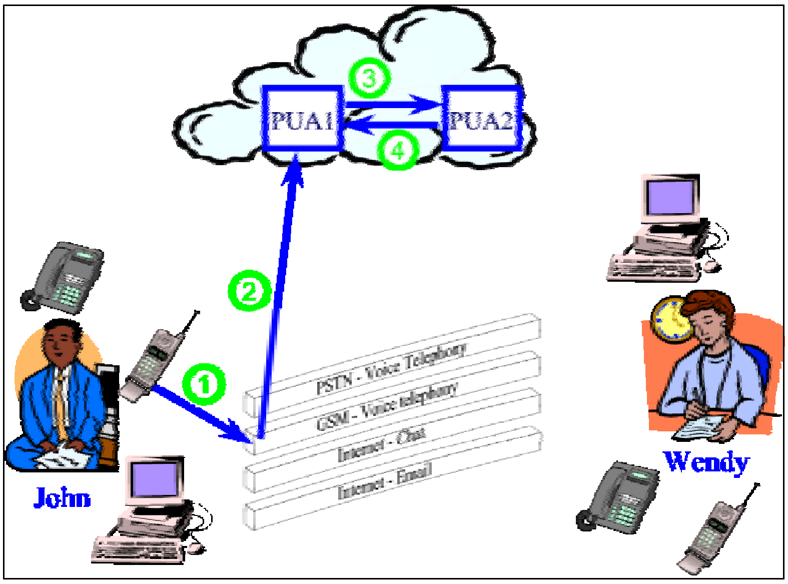


**Figure 5: Negotiating and determining the service specific identifier**

① John accesses his address book and scrolls through to "Wendy". He presses the "send" button.

② The GSM network establishes communication with his PUA and the appropriate data is transmitted identifying Wendy as the desired receiver.

③ John's PUA contacts Wendy's PUA offering a GSM connection.

④ Wendy's PUA tells John's PUA that Wendy is not available for real-time voice communications. It suggests translation of a voice message to email.

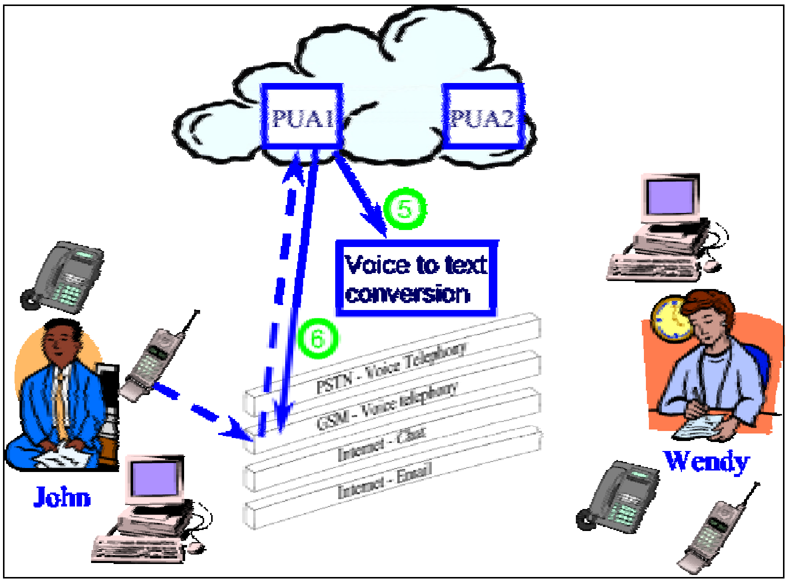


Figure 6: Invoking a voice to text converter

⑤ John's PUA establishes contact with a voice-to-text translation service and gives it Wendy's email address.

⑥ John's PUA communicates to the GSM network the call set up details to the voice to text translation service.

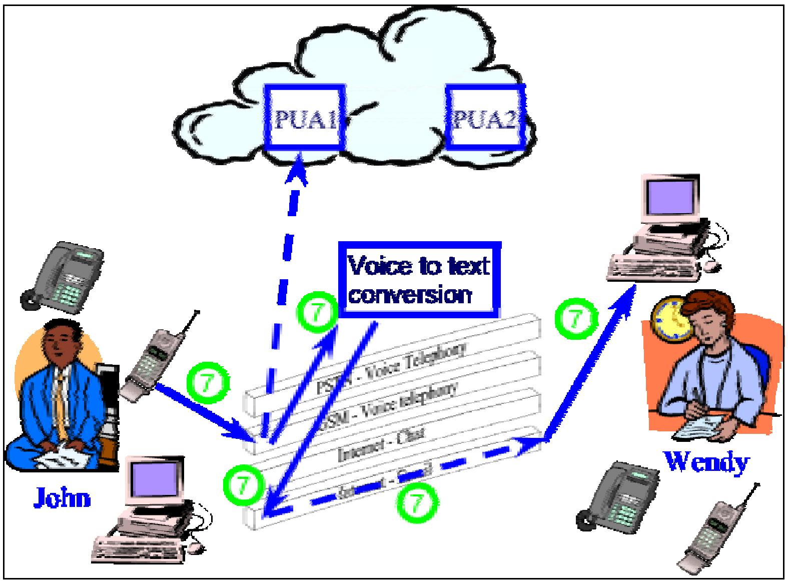


Figure 7: Emailing the receiver via the voice to text converter

⑦ The communication path to the translation service is now set up. John can leave his message that will be delivered via email.

### 10.2.6 Location privacy

When a communication is set-up, the sender does not see the service specific identifier for the recipient as it is sent from the sender's PUA directly to the communications network/service. This ensures that the recipient's location privacy is preserved, as any location information in the recipient's identifier is not seen by the sender. The sender's UCI contains no information on the sender's current location so, when this is sent to the receiver, the sender's location privacy is not compromised. To guarantee the location privacy of the sender and receiver, their PUAs must also ensure that communications networks and services do not send terminal location information. This may mean that the PUAs of the sender and receiver will need to invoke services such as Calling Line Identity Restriction (CLIR) and Connected Line Identity Restriction (COLR) when communications are routed over fixed telephone networks.

## 10.3 Meeting user requirements

### 10.3.1 Uniqueness (R30)

The label part of the UCI, consisting of alphabetic characters, will not be unique but this will not be used for routing through the network(s). The allocation process associated with the UCI means that the numeric string will be unique and therefore that the UCI (numeric string plus alphabetic label) will be unique.

### 10.3.2 Memorability (R31)

The numeric string will inevitably be an almost random set of numbers and therefore difficult to remember. However, users will rarely have to input this string. In most circumstances the users own PUA or their local terminal will contain frequently used numbers indexed by name. Smartcards, PDAs and personal organizers would be other means of porting this information. For those without their own PUA or intelligent terminal, a universal directory search process would enable the establishment of communication whilst inputting memorable data like name, address, date of birth.

In summary although the principle routing component of the UCI (the numeric string) is difficult to remember, sufficient intelligence should exist in the network and the user's terminal to set up a communication by means of the very memorable labels and associated search data.

### 10.3.3 Length (R32)

In practice the numeric string will be the length of a Credit Card number. Its efficiency in representing a globally unique Universal Communications Identifier is high and there will be little redundancy.

### 10.3.4 Stability (R33)

The proposed solution requires the establishment of Certification Authorities which will allocate UCIs either directly or via a Service provider. The data associated with these UCIs such as address, aliases, club membership, could be changed by the user themselves but the numeric string and the authentic information (including the real name) would be unalterable. Major changes such as a name change on marriage would have to be referred back to the Certification Authority although this would still not require any alteration to the numeric string of that user.

The proposed solution is therefore very stable.

### 10.3.5 Terminal independence (R34)

Entry via a 12-button keypad will be possible although only the numeric string could be entered efficiently. It will still be possible to obtain a communication via a voice input of the alphabetic label and other search data to a directories operator.

### 10.3.6 Searchability (R35)

The proposed solution assumes a co-ordinated network of certification agencies providing authenticated and tamper-proof UCIs to a network of Personal User Agents. These UCIs would be associated with user entered details to facilitate search such as address, profession, and date of birth. The directory search facility could be available to all users either by an on-line search engine or via a human intermediary (operator). This facility would search the data from all UCI directories to obtain matches.

### 10.3.7 Robustness (R36)

It is envisaged that most users will maintain a local or network based address book. Sending a communication will therefore entail entering the potential receiver's label name. Thesaurus and error correcting ability to varying degrees could exist within the address book function.

Senders using basic technology (a 12 button keypad) would have to determine and enter the numeric string. This would have the robustness of a conventional telephone number (i.e. none)

### 10.3.8 Meaningfulness (R37)

The addition of the alphabetic label enables the UCI to be ascribed to a person, group or company. Even a basic telephone could access this information given the addition of a small, potentially cheap add-on unit comparable to today's CLI display units. All terminals, however basic, could use a ring-back service (such as 1471 in the UK).

### 10.3.9 Additional information (R38)

Theoretically there is no limit to the amount of extra information that can be sent with the UCI as defined. Current thinking is that the most important need would appear to be the determination of whether the call was from a person, group or business, and whether the name given in a label is the real name or an alias.

### 10.3.10 Authenticity (R39)

Because each standard UCI is allocated by a trusted third-party, it can be considered to be trustworthy by definition. It is not possible to consider user-created anonymous or alias UCIs as trustworthy to the same degree. It may, however, be possible for certain authorized parties, e.g. police authorities, to be able to identify the real identity of the owner of an anonymous or alias UCI.

## 10.4 Comparison with rejected solutions

The "label + number solution" meets the majority of the most essential user requirements to a similar degree to the "Internet URN". Because of its unique feature of separating the meaningful information (the label) from the unique and stable information (the number) this solution is able to maximize the ratings on all of these very important user requirements. The form of identifier also has unique feature of the provision of additional information that is stored and transported with the identifier. The location privacy described in clause 10.2.6 is another feature that is most effectively provided by this solution.

A summary of how the identifiers in the various proposed identification solutions meet the User Requirements for user identifiers described in the present document is shown in table 3.

**Table 3: Comparison of all proposed personal identifiers**

| User Requirements | Directory-based Multi-identifier | Meta-search | Internet Common Name (CN) | Internet URN | Proposed Label + Number UCI |
|---|---|---|---|---|---|
| Uniqueness (R30) | ***** | *** | * | ***** | ***** |
| Memorability (R31) | * | ** | ***** | *** | ***** |
| Length (R32) | ** | *** | ***** | ***** | *** |
| Stability (R33) | * | * | * | ***** | ***** |
| Terminal Independence (R34) | *** | * | * | * or *****<br>see clause 9.4.3.5 | ***** |
| Searchability (R35) | ***** | ** | *** | *** | ***** |
| Robustness (R36) | ** | ** | ** | ** | ** |
| Meaningfulness (R37) | ** | ** | ***** | ** | **** |
| Additional information (R38) | * | * | * | * | ***** |
| Authenticity (R39) | * | * | * or *****<br>see clause 9.3.3.10 | ***** | ***** |
| NOTE 1: ***** Meets requirement extremely well.<br>NOTE 2: * Does not meet requirement. | | | | | |

The only conclusion that can be drawn from an analysis of the rejected proposals and the proposed solution is that the proposed solution clearly meets the widest range of user requirements. A secondary observation is that, the "Internet URN" (clause 9.4) meets sufficient of the user requirements to make it a possible candidate for the "number" part of the proposed solution. At this time it is not clear whether the URN could be practically utilized in this role as part of the proposed solution.

Table 4 shows how the proposed solution (the identifier and its support environment) meets all the requirements associated with an identifier as described in the present document.

**Table 4: Effectiveness of the Universal Communications Identifier (UCI)**

| UCI Element | Requirements met |
|---|---|
| Label | R 31 - Memorability (clause 7.2)<br>R 32 - Length (clause 7.3)<br>R 33 - Stability (clause 7.4)<br>R 37 - Meaningfulness (clause 7.8) |
| Number | R 30 - Uniqueness (clause 7.1)<br>R 33 - Stability (clause 7.4)<br>R 34 - Terminal Independence (clause 7.5) |
| Additional information field | R 38 - Additional Information (clause 7.9) |
| Advanced UCI support architecture | R 35 - Searchability (clause 7.6)<br>R 36 - Robustness (clause 7.7)<br>R 39 - Authenticity (clause 7.10) |

# 11 Implications of the proposed solution

Putting in place the infrastructure and standards to implement the proposed solution might be a complex and expensive process and needs further investigation. Some of the alternative proposals would be less expensive and complex but none really meet user's requirements to the extent that will be necessary in a communications environment of ever-increasing diversity and change.

## 11.1 Universal Communications Identifier allocation and authentication

A crucial element in the success of the UCI scheme is the way in which UCIs are allocated and authenticated. People who receive a UCI need to be certain that the user named in the label field of the UCI is who they say they are (R9, R29) and the initiator of a communication may need to validate that the receiver is indeed the intended recipient (R9, R24). Requirements R26 and R27 imply that there needs to be a way of distinguishing between UCIs related to business roles and UCIs related to individuals. To satisfy these requirements, the following mechanisms are proposed:

General

- Each UCI must be created and assigned by a "Trusted Party";
- Once created, the certified elements of a UCI must be in a form in which any attempt to alter the UCI will make it invalid;
- All UCI owners will be free to create UCIs in which the label component is anonymous or an alias;
- User created anonymous or alias UCIs will contain the same numeric string as the certified original UCI but will be flagged as anonymous or an alias.

UCIs for individuals

- Each UCI for an individual must be created and assigned by a trusted public body;
- All UCIs for individuals will contain information in the additional information field that identify them as UCIs for individuals.

Corporate UCIs

- Each company must be certified by a trusted public body;
- Companies will be able to create, allocate and have responsibility for UCIs that represent roles within their company (i.e. a public body certifies the company and the company certifies the roles within it);
- All UCIs created by a company will contain information that cannot be tampered with that accurately identifies the company;

- All corporate UCIs will contain information in the additional information field that identify them as corporate UCIs;
- Corporate UCIs may contain the name of an employee in their label field.

The way in which the trusted bodies are chosen or created may vary significantly from country to country and over time. It is not within the scope of the present document to attempt to prescribe how such bodies should be set-up. Issues such as the legal status of companies and the circumstances under which a body can be certified as a company capable of issuing its own UCIs is also a matter that is outside the scope of the present document.

A global set of agreements and standards that will ensure that a level of trust exists in the system that is compatible with the security requirements of basic person-to-person communication are required. The X.509 [5] recommendation describes a model of public and corporate authentication that may be a good basis upon which a suitable UCI authentication mechanism can be built. For certain transactions carried out over communication channels (e.g. e-commerce), a level of trust higher than that needed for basic communication may need to be established. It is expected that additional or extended security mechanisms will need to be put in place to enable higher trust relationships to be established.

## 11.2 Information Records

To satisfy User Requirements R8 and R15 there must be an information record associated with each UCI. The UCI, which is the address of the individual's PUA, would be one attribute of an information record. Several UCIs (e.g. an "authentic" UCI and one or more alias UCIs) may be associated with a single information record.

The information record should be updateable by the individual. The only attributes that cannot be simply and directly updated are the numeric fields of the UCIs and the authentic label text of the authentic UCI (e.g. the authentic name of the individual or role). To update the authentic label, a new certificated authentic label would have to be obtained from the certifying authority and transmitted to the body that manages the person's information record.

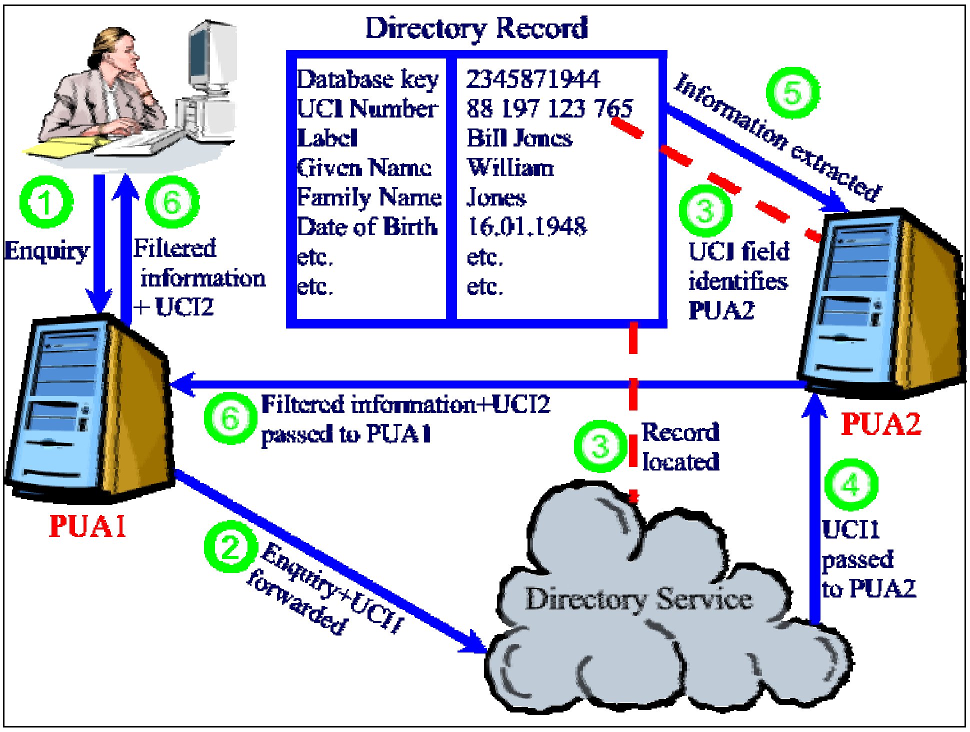
Standardized groups of attribute types would be needed for all information records, and these would need to include such items as the authentic label and basic identification information such as name and date of birth. An ability to allow the range of attributes to be modified and extended is required to ensure that, as the range of important factors changes over time, the information record attributes can easily be changed to reflect these changes (e.g. if the initial set of attributes had been designed in 1980, a field for Web site address would not have been included, but this would now be considered essential). The XML concept of attribute spaces (see "Recommendation: Namespaces in XML", annex G) is one possible mechanism that could be used to provide this flexibility.

In order to avoid data duplication, with the associated dangers of data inconsistency, Personal User Agents will need to use information records as the exclusive source of the information they need to process or communicate.

## 11.3 Directories

In order that Requirement R15 (Determining a personal identifier (if unknown) by means of a directory search process) can be met, there is a need for a global directory service. In order to avoid data duplication, with the associated dangers of data inconsistency, the global search mechanism will need to use information records as its exclusive source of information to query or to communicate. However, the directory could also include entries for people who do not have UCIs. Where the directory entry is an information record, as described above, the essential piece of information that would be returned to an enquirer is the UCI that forms the address of the person's PUA.

In order that Requirement R7 (Privacy) can be met, it is necessary for the user's desired level of privacy to be reflected in terms of the amount of information that is returned to the enquirer. The owner of the UCI may wish to vary the amount of information that can be released dependant on the identity of the enquirer (if known). In order to carry out the user's wishes, it is necessary that the user's PUA, which is the entity that has been given knowledge of the user's requirements, is involved in the process. One possible method by which all of the requirements could be met is illustrated in figure 8.



Directory Record

| | |
|---|---|
| Database key | 2345871944 |
| UCI Number | 88 197 123 765 |
| Label | Bill Jones |
| Given Name | William |
| Family Name | Jones |
| Date of Birth | 16.01.1948 |
| etc. | etc. |
| etc. | etc. |

**Figure 8: Possible mechanism to allow user control of privacy in directory searches**

Figure 8 illustrates a possible mechanism by which directories might be accessed.

① An enquiry is made prior to a communication.

② The UCI of the enquirer and the enquiry are communicated to the Directory Service.

③ When a successful enquiry has been made and the Directory Record of the intended receiver is found, the UCI in that record enables the person or organization's PUA to be identified.

④ The PUA of the intended receiver (PUA2) receives the identity (UCI) of the enquirer (UCI1).

⑤ It extracts all the data from the information record.

⑥ The intended receiver's PUA then decides what information should be returned to the enquirer and sends this filtered information, together with its own UCI to the enquirer via the enquirer's PUA. If the privacy requirements of the intended recipient state that they do not wish their UCI to be presented to the enquirer (so that the enquirer is prevented from storing their identity), the PUA of the enquirer is instructed not to forward the returned UCI but to use it solely for the purposes of establishing a call.

## 11.4 User Interface

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.

The present document does not provide specific recommendations on the user interface to the communications control environment. However, the following areas are highlighted as those in which particular care is needed to ensure that the overall environment is usable.

### 11.4.1 Communications set-up

Communications will be initiated on a wide range of terminals; from a basic 12-button telephone to a full graphics capability device. The sender of a communication must be able to:

- access their address book;
- specify a preferred service;
- assign urgency.

The challenge to the user interface designer will be to allow the full power of the UCI/PUA based communications to be available whatever the terminal type.

### 11.4.2 Incoming communications information

Use of the UCI offers the opportunity for information relating to the incoming communication to be available at the receiver's terminal. The information would normally be displayed on screen or display, but could be presented aurally on basic terminals. User interface designers will have to decide just how much information is presented and allow the receiver an appropriate response if required.

### 11.4.3 Communications management

This is the most critical of all the user interfaces. Many attempts to offer incoming communications management as a commercial package have failed because of poor user interfaces. Where a poor interface is supplied, users see the task of maintaining their communications filtering/re-routing configuration as a chore where the payback is not worth the effort required. If the user interface is not usable (efficient, effective and a delight to use) then the UCI will not be used to full effect. The interface needs to allow the user:

- to check the current configuration;
- to edit the existing configuration.

It is most probable that users' will access their communications manager via an IP network that will allow the use of a relatively sophisticated user interface. Additionally, modern architectures and technologies will enable some management control to be automatic. In particular, GSM and derivative mobility functions enables a user's movements to be tracked and their communications routed accordingly. A graphical interface with semi-automatic updating will only go part of the way however. A great deal of thought, flair (and task analysis) will be needed to design a user interface to show, in a simple way, very complex time-dependent configurations and to allow those configurations to be easily edited.

### 11.4.4 Directory search strategies

Unlike most currently available directory services, a UCI based directory service will allow searches based on a wide range of attributes. For instance I may know that John Smith is secretary of Coventry Tennis Club and is interested in model engineering. This information could easily be included in John Smiths directory record. The user interface may have to allow this flexibility of input on a wide range of terminals.

### 11.4.5 Verification

Senders and receivers of communications may be able to request verification of receiver and sender respectively. The user interface must support this requirement on a range of terminals. Unambiguous identification of the user at the terminal they are using needs be as unintrusive as possible. Biometrics may play a key role here in the future.

### 11.4.6 Presentation of UCI (on paper)

A great deal of thought has been given to the presentation of telephone and fax numbers on paper and business cards. There is an ITU Recommendation on the subject [10]. Similar consideration needs to be applied to the presentation of UCIs on paper and business cards.

### 11.4.7 Presentation of communications history

Presentation of communications history should be reasonably straightforward in user interface design terms. As a minimum users will almost certainly require the ability to specify how much information is provided about each communication and to have alternative "views" of the history e.g. by date or by sender.

## 11.5 Identification

In any environment where a communications terminal is regularly used by more than one user (a shared terminal), the problem of identification of a specific person is an issue, whatever form of Identifier is used. In fact most homes and offices will experience this limitation to some extent. In a home, for instance, each family member would have a different UCI and some members of the family might use different Personal User Agents.

### 11.5.1 Identification of sender

When wishing to set up a communication from a shared terminal, the user needs to contact the PUA and tell it who is making the communication. This should involve as little effort on the part of the user as possible. Some currently proposed systems involve keying or typing a code before each communication. However, this could become tedious and be a barrier to the adoption of such advanced systems.

Some email systems, where several members of a household share a common access, already address this problem. When sending an email in this case, the user is presented with a menu from which to select the identity of the sender. The problem here is that if this is omitted by mistake the default sender is assumed and this could potentially lead to some confusion.

Many shortcuts could be envisaged which would establish contact with the PUA more or less instantaneously:

- use of a personal smartcard for each regular user (with a smartcard reader on each terminal);
- use of dedicated access keys on a terminal for each regular user;
- biometric methods - Speech recognition; face recognition, iris recognition, fingerprint identification, etc.

As current software companies are beginning to build smartcard and biometric user identification capabilities into their operating systems, these currently costly and complex options may soon become more freely and cheaply available.

### 11.5.2 Identification of receiver

Given the fact that anybody using a UCI wishes to access a person and not a terminal it will be important that the communication is "delivered" to the right person. Store and forward services are not so much of a problem as the communication is placed in the receiver's mailbox. For real-time communications an indication of the intended receiver is required at the shared terminal. Future systems could provide:

- the intended receiver's name on a display;
- personalized ring-tones.

## 11.6 Verification

The ideas outlined above do not provide any sort of verification of who is sending or receiving a communication. Extra procedures will be required to meet requirements R24 and R29. This will entail additional dialogue and signalling support between the two PUAs.

### 11.6.1 Verification of sender

The receiver may require confirmation that the sender **is** the person indicated on their display and would activate a verification process via a dedicated terminal key (GUI or physical) or a code. The receiver's PUA would ask for verification of the sender from the sender's PUA. The sender's PUA would either already know that the sender was who they claimed to be, because one of the biometric or smartcard recognition processes outlined in 11.5.1 had already been carried out, or it would ask for a PIN.

### 11.6.2 Verification of receiver

Verification of receiver may be requested when setting up the communication. The receiving PUA would then request confirmatory ID from the individual who answered the call. These could be:

- use of a personal smartcard;
- a PIN;
- biometric methods (see clause 11.5.1).

Once the receiver's PUA had verified the receiver as the right person this would be communicated back to the sender via the sender's PUA.

## 11.7 Efficiency of communications set-up

At first sight the use of Personal User Agents and UCI appears as if it could lead to inefficient use of the network, particularly when the same communication is being made on a regular basis. For instance, under current telephony systems, a simple number is input which routes the sender directly to the receiver's telephone. Under the proposed system it would appear that for each communication, however straightforward, there must be a dialogue between PUAs before the communication is established. This need not be the case however. The PUAs could be intelligent enough to detect that the same service specific identifier (SSI) is being regularly returned and maintain a cache of frequently used SSIs (with a built-in time-out). Alternatively a receiving PUA might "say" to a regularly sending PUA "look, use this SSI for voice communication between 9 am and 5 pm, if there is any change I will contact you and let you know the new arrangements". Either way means that the pre communication dialogue between PUAs is rendered unnecessary in regular simple communications. The Personal User Agent is becoming, to all intents and purposes, a personal assistant doing everything that a human personal assistant might be expected to do.

# 12 Benefits of the proposed solution

When UCIs and the systems underlying them are deployed many parties will derive benefits. In this clause, some of the potential benefits of a UCI system are described. The different parties identified below are logically separate, but in practice a single organization could fulfil the role of more than one of these parties (e.g. a single organization could supply communications services and provide PUAs).

One key benefit of the UCI that impacts on all the parties listed below is that the UCI is completely service independent and it can thus be used by the senders and receivers of communications for all future services as well as for all present ones.

## 12.1 UCI owner

As a UCI owner you will get:

- greater selective control over who contacts you, how they contact you (realtime, messaging, voice, text, etc.), at what times and on what terminals they reach you;
- a better guarantee that those whom you want to contact you can do so with ease;
- an opportunity to publicly register your identity if you own a non-subscription terminal (e.g. pre-pay mobiles). This may be done in a selective way so that only some people can access your identity.

## 12.2 Person contacting UCI owner

As a person contacting a UCI owner you will get:

- better communication success if the person you are contacting wants to communicate with you;
- your communication attempt handled more gracefully if the person doesn't want to talk with you now (e.g. you will be allowed to leave a voice message and your UCI);
- a global directory service to acquire an identifier for a new contact;
- use of a single efficient address book function that allows you to communicate with UCI owners across all services.

## 12.3 Communications service/application suppliers

As a supplier of communications services or applications you will get:

- a greatly increased number of successfully completed communications (including termination of real-time communication attempts on voice/text messaging systems) leading to:
    - increased customer satisfaction for senders and receivers of communications resulting in greater customer loyalty;
    - increased revenue from the extra communications.
- more people subscribing to new services as they will not be inhibited by a reluctance to acquire yet another identifier.

## 12.4 Terminal manufacturers

As a terminal manufacturer you will get the opportunity to sell new terminals that incorporate:

- UCI capture facilities;
- local label editing facilities;
- smart interfaces to directory services;
- facilities to synchronize local address books with a centrally held address book;
- smartcard reading;
- biometric recognition capabilities.

## 12.5 Providers of new functions

In the proposed solution there are a number of functions that need to be provided such as:

- the issuing of UCIs;
- the provision of PUAs;
- the management of personal data;
- the provision of directory services.

It is possible that each of these functions could be provided by separate suppliers or, alternatively, a single supplier could provide most or all of these services. Because of the potential variations that might exist it is not possible to detail all of the benefits that might accrue to the suppliers of these functions. One thing that can be said is that there is potential for a very open and competitive market in the supply of these of these functions.

It is important that the issuing of UCIs is not seen as a high-value competitive area as an essential component of the proposed solution, or any solution meeting the user requirements, is stability of the UCI. One option for achieving this might be for a non-profit making national body to issue UCIs. Another alternative is to allow the providers of other services or functions to issue UCIs with the understanding that the UCI cannot bind its owner to those services or functions.

### 12.5.1 PUA provider

As a PUA provider you will get the opportunity to:

- provide software capabilities that allow the user to precisely match their needs when making and receiving communications (tailorability);
- offer different packages that can range from expensive solutions providing every different capability to much simpler and cheaper packages that offer only a basic range of services.

# 13 Migration

From the initial conception of the UCI scheme, it has been assumed that it would be able to be implemented as an overlay to existing and future networks. Where the UCI system is not implemented, the existing networks would operate exactly as they do at present, using the identifiers that are currently used (e.g. telephone numbers and email addresses). Where the UCI system is introduced, there would be two possible ways of using the underlying communication systems.

It is worth exploring two stages:

- a single island of the new UCI solution;
- multiple islands of the new UCI solution.

It is assumed that, as at present, there will always be places in the world where the communication technologies are one or more generations behind. Hence the option of a 100 % UCI implementation worldwide is not worth discussing as a useful scenario upon which to plan any streamlined complete communication environment.

In the first instance, where one organization offers a UCI solution to people who wish to participate, all those people who subscribe to this organization's service will be able to derive the maximum benefit from the system. These subscribers will be able to:

- establish contact with other subscribers to the UCI system using all of the methods inherent in the UCI system (recall from local UCI store, doing a search for the intended receiver and direct entry of the receiver's UCI);
- identify any fellow subscriber to the UCI system who contacts them;
- capture the identifier of any fellow UCI system subscriber who contacts them;
- effectively identify themselves to other subscribers who they contact;
- establish contact with fellow UCI subscribers in the knowledge that their communication requirements will be met in the most effective way;
- very effectively manage the way they handle communications from other UCI system subscribers;
- manage communications from non-UCI system subscribers in a more limited way.

Non-subscribers calling these UCI system subscribers will obtain very few benefits. They should however have an enhanced chance of contacting the UCI subscriber because of the help provided by the subscribers Personal User Agent.

Where there are multiple islands of the new UCI solution, two possible outcomes may arise. If no attempt is made to standardize the ways in which these islands intercommunicate, then the benefits obtained by the subscribers will be those stated above. If the multiple islands are able to interchange UCI information, then the multiple islands effectively become a single larger island and the benefits described above will apply to the enlarged group of subscribers.

Clearly, to be anything more than a limited local (or at best national) service, a range of standards issues will have to be addressed. These will be covered in clause 14.

# 14 Required standards and agreements

It is possible to deliver all (or most) of the user requirements described in the present documents when many aspects of the systems to support UCIs exist in a competitive environment. Businesses would be free to develop alternative competing solutions in a number of areas, including:

- the internal design of Personal User Agents and their user interfaces;
- the detailed user interface design of terminals and end-user applications.

Such competition would stimulate innovation and variety. This would bring significant benefits to end-users in allowing them to choose a product or service that met their own personal needs at an acceptable price.

In contrast, there are a number of areas where standards and agreements would be necessary in order to allow an environment for handling UCIs to function at all. Four specific areas are described below.

## 14.1 UCI format

In order that all of the separately developed components of a UCI handling system can effectively interchange and process UCIs, the format of the UCI must be standardized. The description of the UCI within the present document forms a basis on which standards could be developed. These standards would have to specify more fully the size and content of the various elements of the UCI, the handling of multiple alphabets and also define the process(es) by which UCIs would be allocated. The definition of the IETF vCard [9] may also provide valuable input into the development of the more detailed standards needed for UCIs.

Within ETSI, the most appropriate body to consider this standardization would appear to be SPAN2. However, a global solution could only be achieved with global standardization and hence, in addition, standardization would be needed by joint agreement between the IETF and the ITU-T.

## 14.2 UCI resolution service

Every UCI is associated with a PUA that manages communications on behalf of the person or organization to which the UCI has been assigned. In order that the appropriate PUA is reliably located each time that a UCI is used, a resolution service is needed to resolve each UCI to the address of the associated PUA. As it is probable that communication between PUAs would take place in the Internet domain, the IETF would be likely to be the lead body in the specification of this UCI resolution service. Given the major link to telecommunications services, it would be necessary for the specification of the resolution service to be carried out in collaboration with the ITU-T, 3GPP and ETSI.

## 14.3 PUA intercommunication

Although the software design of PUAs should be a matter for free competition, there are two areas that need to be standardized or upon which global agreements need to be reached:

- the content and protocols for intercommunication between PUAs;
- the establishment of an environment of Trust between PUAs.

Consideration of agent communication in a communications context took place within the TINA (Telecommunications Information Networking Architecture Consortium) consortium (www.tinac.com). Current work on evolving standards to define agent interoperability is taking place in FIPA (Foundation for Intelligent Physical Agents) (www.fipa.org). In the context of inter-operating PUAs, the most appropriate bodies to lead standardization efforts would appear to be some form of joint work between ITU-T Recommendation SG.13 (see annex G), the IETF and 3GPP, taking account of specifications emerging from FIPA.

## 14.4 Directories

To satisfy several of the user requirements, a global directory search mechanism would be needed. In order for such a directory search mechanism to be implemented there would need to be standards that covered such aspects as:

1) a standard query interface and data interchange mechanism for use by software applications (it is assumed that the query interface to end-users would be subject to competition);

2) the hierarchical structure of databases and the handling of database distribution;

3) the basic attribute sets of database records and the mechanisms by which these can be extended or modified over time;

4) the minimum functionality that an end-user interface must provide to allow end-users to successfully locate UCIs.

Existing standards form a very solid basis on which the above standards could be developed. In particular, the ITU-T Recommendation X.500 series Recommendations [3], [4], [5], [6] cover many of the above issues and work taking place in the IETF is evolving standards that also cover these issues. Several of the developments taking place in the use of XML tackle issues of data interchange between heterogeneous databases, the ability to define and use multiple attribute sets (XML Namespaces, see annex G), etc.

The existing collaboration between the ITU-T and the IETF in the area of directories forms a good basis upon which the proposals in the present document can be supported.

# Annex A (informative): Summary of user requirements

This annex summarizes the user requirements derived throughout the Guide.

# A.1 User requirements

## A.1.1 Generic (high level) requirements

**User requirement No R1 - Unifying the control of communications (clause 5.1)**

Users require a universal identifier and a unified method of, and support for, setting up, receiving and managing communication that is, as far as possible, independent of the terminal(s), application(s) and service(s) used.

**User requirement No R2 - Reducing the impact of network boundaries (clause 5.2)**

Users require seamless communication across networks and services.

**User requirement No R3 - Increasing the options available to the sender (clause 5.3)**

The sender of a communication requires the ability to indicate to the system particular requirements relating to the outgoing communication.

**User requirement No R4 - Increasing the options available to the receiver (clause 5.4)**

The receiver requires the ability to control which communications are routed where, under what conditions and at what time.

**User requirement No R5 - Dealing with communications conflicts between sender and receiver (clause 5.5)**

Users require that conflicts between the communication requirements of the sender and the receiver should be resolved, where possible, without their intervention.

**User requirement No R 6 - Maintaining backward compatibility (clause 5.6)**

Even with future architectures, users may wish to use basic input devices such as a 12-button numeric keypad to obtain a basic level of service.

**User requirement No R 7 - Providing privacy (clause 5.7)**

Users will require varying levels of privacy including location privacy.

**User requirement No R 8 - User control of personal user agents (clause 5.8)**

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 and that they should always have the ability to prevent the Personal User Agent from carrying out actions that they do not wish to happen.

**User Requirement No R 9 - Trust (clause 5.9)**

Users need to be able to trust that the party described by the identifier is the party with whom communication takes place.

## A.1.2 Communication control requirements

**User requirement No R 10 - Providing communication configuration status (clause 6.1.1)**

Users may require an indication of communication configuration status at any given time.

**User requirement No R 11 - Editing the communication configuration (clause 6.1.2)**

Users require the ability to easily edit their communication configuration.

**User requirement No R 12 - Maintaining communication records (clause 6.1.3)**

Users may require a full communication history to be delivered.

**User requirement No R 13 - User location monitoring (clause 6.1.4)**

Users may require their communications to be effectively managed in relation to their current location.

**User requirement No R 14 - Access to personalized list of known Universal Personal Identifiers (clause 6.2.1.1)**

Users may require an address book of user identifiers to be maintained. They may require this information to be duplicated in more than one physical or virtual location.

**User requirement No R 15 - Determining a personal identifier (if unknown) by means of a directory search process (clause 6.2.1.2)**

Users require access to a directory (or directories) of personal identifiers.

**User requirement No R 16 - Selecting communication medium and characteristics (clause 6.2.1.3)**

The user may require the ability to select a communication medium as their first choice and specify attributes associated with that medium.

**User requirement No R 17 - Establishing contact where possible (clause 6.2.1.4)**

Users may require that, when necessary, alternative options are tried in order to maximize the possibilities of them establishing communication (subject to any overriding requirements of the sender or receiver).

**User requirement No R 18 - Acknowledging social protocols (clause 6.2.1.5)**

Users will require that relevant social protocols be reflected in the establishment of their communications.

**User requirement No R 19 - Providing cost information (clause 6.2.1.6)**

Senders of communications may require that tariff information is made available to them so that they can predict the cost of a communication. Alternatively they may require that the accumulating or final cost be presented.

**User requirement No R 20 - Assign priority to communication when necessary (clause 6.2.1.7)**

Senders will require the ability to assign "urgency" to any communication.

**User requirement No R 21 - Using the senders alphabet (clause 6.2.2.1)**

Senders require their identities to be presented using the alphabet in which their identity is normally presented on paper, where the receiver is capable of displaying that alphabet.

**User requirement No R 22 - Providing sender anonymity (clause 6.2.2.2)**

Senders require the option of anonymity when establishing a communication.

**User requirement No R 23 - Using an alias (clause 6.2.2.3)**

Users may require the option of assuming an alias.

**User requirement No R 24 - Validating receiver identity (clause 6.2.3.1)**

Senders may require the ability to request the validation of the identity of the receiver.

**User requirement No R 25 - Identifying sender (clause 6.3.1.1)**

A user requires the ability to unambiguously identify the sender of a communication or to be told that the sender is withholding their name or using an alias.

**User requirement No R 26 - Barring incoming communications from specified senders (clause 6.3.1.2)**

A user may require the ability to bar communications from selected senders.

**User Requirement No R 27 - Managing incoming communications (clause 6.3.1.3)**

The receiver requires the ability to configure routing and filtering for incoming communications.

**User requirement No R 28 - Awareness of costs (clause 6.3.1.4)**

Users require the provision of costing information on different routing/filtering configurations.

**User requirement No R 29 - Validating the sender's identity (clause 6.3.2.1)**

Receivers require the ability to request the validation of the identity of the sender.

## A.1.3 Identifier requirements

**User Requirement No R 30 - Uniqueness (clause 7.1)**

Users require a user identifier that uniquely identifies a person, role or group.

**User Requirement No R 31 - Memorability (clause 7.2)**

Users require that part or all of the user identifier is easy to remember.

**User Requirement No R 32 - Length (clause 7.3)**

Users require the user identifier to be as short as possible.

**User Requirement No R 33 - Stability (clause 7.4)**

Users require that user identifiers are permanently allocated to a single person, role or organization.

**User Requirement No R 34 - Terminal Independence (clause 7.5)**

Users require the ability to enter a user identifier on a basic 12-button numeric keypad connected to any type of network.

**User Requirement No R 35 - Searchability (clause 7.6)**

Users require the ability to search for and find the user identifier of "listed" users.

**User Requirement No R 36 - Robustness (clause 7.7)**

Users require that when common mis-spelling and keying errors are made when entering a user identifier the systems it is used with should be able to cope.

**User Requirement No R 37 - Meaningfulness (clause 7.8)**

Users receiving communications require user identifiers that contain the name of their owner - either a person, organization or a role.

**User Requirement No R 38 - Additional Information (clause 7.9)**

Users wish to be able to determine whether a communication is from a business or private source and whether the sender is remaining anonymous, communicating under an alias or using their correct name.

**User Requirement No R 39 - Authenticity (clause 7.10)**

Users require identifiers that contain information that they can be sure will always accurately describe the owner of the identifier.

# Annex B (informative): Future scenarios

All the examples below will assume that innovative network architectures and Universal Communications Identifiers have been around for many years and the penetration is high. Both sender and receiver use Personal User Agents for most of their communications. In these scenarios, PUA(r) refers to the receiver's Personal User Agent. The underlying communications services described in these scenarios are based upon current communications services, and no attempt has been made to predict future communications services.

# B.1 Future scenario 1 - Establishing contact

You want to get in touch with the secretary of the local tennis club (who lives in Antibes and whose name is John) to get subscription details:

- you call up your PUA via on-screen menu and direct it to find the UCI of the intended receiver given first name (John), role (secretary tennis club) and location (Antibes);
- your PUA displays to you that the UCI has been found and gives you the option to store it in your address book;
- you request voice connection (by pointing to appropriate button on screen);
- your PUA contacts PUA(r) to request voice connection;
- PUA(r) informs your PUA that no voice connection is available (John is out playing tennis) and offers either:
    - a voice mailbox; or
    - voice note by email; or
    - typing an email;
    - automated translation voice to fax; or
    - automated translation voice to email;
- your PUA already knows that your preference in the absence of direct voice contact is translation to email output when available and establishes appropriate connection path;
- your PUA requests you to leave message via microphone in-built into the terminal;
- John returns home and finds email requesting subscription details and will now have your UCI automatically shown on the email and stored in his personal address book ready for the return communication.

# B.2 Future scenario 2 - Filtering and re-routing

You are a consultant dividing your time between one client in London and another in Sophia. Your PUA maintains a diary updated from your Personal Organizer of where you are likely to be and when. Your comms configuration is set up for the re-routing of **all** communications received to one site or another (or your home at weekends and evenings). A deliverable is now due so you must do something about all those time consuming communications. You must also spend the next few weeks working permanently in Sophia. You decide only to accept communications from close family and from your other client plus any unforeseen emergency calls from your family/friends.

- You contact your web-based PUA and call up the comms configuration overview page. This gives you a graphical indication of your comms structure with re-routing and filtering conditions shown.
- You click on the re-routing box which currently displays "all" and now select "special conditions".

- You now go through various multiple select menus which enable you to impose conditions on the re-routing and select from predefined groups in your address book.
- Thus you select for re-routing all communications from your immediate family, from your major client, or communications flagged as urgent from friends. In all these cases the source will be determined by your PUA from the senders UCI.
- You call up the comms configuration overview page again to check that all is as it should be then click on "OK".
- You forgot to tell your PUA that you would be in Sophia for a while but it does not matter.

  Your PUA will know exactly where you are because your GSM phone and your terminal logins will eventually provide this information. The PUA therefore tells you that it will be routing all selected communications to your site in Sophia unless instructed otherwise.
- You meet your deadline with the help of effective communications management.

# B.3 Future scenario 3 - Anonymity

You want to contact your local car dealership to enquire as to the cost of a new car but you don't want the dealer ringing you back, pestering you.

- You call up your PUA via on-screen menu and direct it to find the UCI of the intended receiver giving the keyword "car dealer X" and a location of "Ipswich".
- Your PUA displays that the UCI has been found and gives you the option to store it in your address book.
- You request voice connection (by pointing to appropriate button on screen) and request anonymity (by pointing to another button).
- Your PUA contacts PUA(r) to request voice connection and indicates that no UCI will be sent.
- The car dealership is familiar with anonymous communications and has authorized its PUA to receive them. PUA(r) therefore gives your PUA the necessary data to set up the call and you are put through.
- You speak to the salesman and receive the information you are after but are not pestered afterwards by follow-up calls from the dealership.

# B.4 Future scenario 4 - Universal terminal capability

The full functionality and power of the new communications capabilities enabled by the use of UCIs is normally accessible by using your Web-based communications controller. Often however it is necessary or more convenient to use more basic communication devices. Manufacturers now supply very sophisticated extension phones, mobiles etc which fully support the new architectures, some with full colour displays and alpha keyboards. You are due to play golf in 2 hours and are washing your car with a cordless telephone clipped to your belt.

- It gives a distinctive ring (Beethoven's Fifth- opening chords) meaning the call is for you, and not for your wife.
- You look at the display. It shows an urgent flag and is from your friend John Jones.
- John tells you he is delayed by one hour; can you re-arrange the golf match?
- You press the Personal User Agent key on your cordless. Most of the PUA functionality is now accessible.
- You press the "address book" function on your cordless and scroll through (alphabetically) on your small display until your other golf partner Fred has been selected.
- You select "connect". Your PUA assumes you require voice connection because of the terminal type and you are offered mobile voicemail, or translation voice to fax or translation voice to email (John is obviously unavailable)
- Because of the urgency you select all three and send your message.

- You now need to contact the Golf Club so you press the Directory Service key. Because the PUA knows you have no alpha keyboard, it connects you to a human operator (maybe speech recognition technology one day).
- The operator retrieves the number for you and downloads the details to your PUA.
- The golf club is now in your scrollable address book and can be easily accessed to change your arrangements.

# B.5 Future scenario 5 - Security

You are surfing the Internet looking for an antique vase and see one illustrated in the catalogue of a dealer in Bruges.

- The UCI of the dealer is captured and stored in your address book.
- You access your Web-based communications management page and request a voice connection to the dealer.
- The deal is made by voice over the telephone and the dealer requires official confirmation and deposit within six hours (he has somebody else trying to buy the vase).
- You select his UCI and indicate that you want to send an email with "special conditions".
- You select "improved security communication" because credit card details will be sent.
- You select "confirm receiver" for peace of mind. This will give you a confirmatory message once the email has been delivered and confirm that it has been sent to the correct recipient.
- You send you email with the card details. 30 minutes later a confirmatory message arrives.
- The antique vase is yours!

# B.6 Future scenario 6 - Privacy

With the new Universal Communications Identifier system, individuals can assume aliases but the usage of an alias is always labelled as such in the "additional information" field.

You currently allow all incoming communications to reach you whether they are anonymous, alias or real, but have recently had many irritating voice communications from people not disclosing their real names.

- You access your Personal User Agent web page and call up a communications history. You notice that there have indeed been 7 voice calls in the last 10 days from people using aliases. All of these as far as you can remember were from people and companies trying to sell you products you did not want. You have also had several alias calls via email but it is common practice on some of your egroups to use nicknames and these are quite acceptable. You are also reminded by examining your comms history that there have been several annoying calls from people using their real names. You decide to decrease your accessibility.
- you contact your web-based PUA and call up the comms configuration overview page. This gives you a graphical indication of your comms structure with re-routing and filtering conditions shown.
- There is a filter box for each service you use and you click on the top level "filter PSTN" box which brings up a range of filter "tick boxes".
- You now deselect the ticks in the "alias" and "anonymous" tick boxes and click on the "OK" button.
- You click on the directory "privacy" box.
- Options are now displayed ranging from "no access to UCI by directory search" through to "any directory searches to be referred to you for acceptance".
- You click on a box labelled "available to anybody already in my address book".

All PSTN voice calls which are not labelled with a real name will now be barred but mobile calls, emails with aliases are still delivered to you. Nobody will be able to ascertain your UCI accept those people who you already communicate with and those you have given it to (e.g. on a business card).

# Annex C (informative): The current environment

# C.1 Identification schemes

## C.1.1 E.164 Telephone numbering scheme

In current telephony systems, the use of telephony numbering based on the ITU-T Recommendation E.164 is universally adopted. The E.164 Recommendation defines three different types of number:

- Geographically dependent number - where a country code is part of the number and all the numbers assigned to that country code are managed by that country (including service related numbers e.g. freephone numbers);
- Global service numbers - for specific services that are available globally, currently - Universal International Freephone (UIFN), Universal International Shared Cost Number (UISCN); Universal Personal Telecommunication (UPT); and Universal International Premium Rate Number (UIPRN);
- Networks - For International Networks that meet specific criteria (in E.164.1) a country code (currently 881 and 882) and 1 or 2 digit Identification Code are assigned.

Geographic numbers were originally assigned by monopoly telephony operators. This was a simple but somewhat rigid allocation process. As the telephony market has evolved, telephone numbers are now allocated by a number of telephony providers in each country and number portability between providers is expected. The current situation is now quite complex, with one organization allocating the number and another billing the customer. Different ranges of numbers also assume different meanings related to different types of networks (e.g. fixed or mobile) and different types of charging structure (e.g. local rate, freephone or premium rate). As the range of service type options and charging mechanisms grows rapidly, it becomes increasingly impractical to rely on differing numbering ranges to convey clear information on topics such as charging. It is likely that alternative mechanisms for indicating charging will soon be developed.

A strength of geographic numbers is that one or more of them is associated with every person who currently possesses a device connected to a telecommunications network. As such, they perform a significant role in how we currently contact people in a global context. However, they have several significant disadvantages as user identifiers:

- they are most commonly assigned to communications terminals (or SIMs) and not to people;
- as the number of telecommunications users and the number of services increases, the length of telephone numbers has increased over the years. As number length increases, people have greater difficulty in recalling numbers and holding them in their short-term memory. This issue is discussed in more depth in EG 201 795 [1], where some experimental results of decreasing human performance with number length are reproduced;
- they do not contain any information that, to someone unfamiliar with the number, uniquely associates the number with the person to whom the number has been allocated. They may contain information that gives some idea of geographical position, but this is increasingly negated by number portability;
- their geographic nature means that if a person moves to another country they must acquire a different telephone number. If number portability across national boundaries existed, then this would also pose problems for users, as the number would give misleading information about the true location of an individual. However, this level of confusion already exists in the mobile communication market, as the number that is assigned to a mobile telephone gives no indication of its actual location. This can lead to callers inadvertently causing the person they are calling to incur expensive international call charges;
- global service numbers and numbers from the "Network" ranges do not suffer from the limitation that they tie the owner of the number to one specific country. However, they share most of the other disadvantages of the geographic numbers.

## C.1.2 Internet naming and addressing

In the Internet world, a set of open standards describe current and proposed numbering, naming and addressing methods. Some of these are discussed in the following clauses.

### C.1.2.1 IP Addresses

The lower level identification methods such as Internet Protocol (IP) addresses are hierarchical, very flexible, but unsuitable as vehicles upon which a personal identification system could be based. Three strong arguments that make IP addresses unsuitable are:

- they are numeric and contain no information that has any meaning to most users;
- under the current IPv4 scheme there is a very definite limit to the number of addresses that may be allocated. This limit may prove too small as the number of entities needing addresses continues to increase;
- IP addresses identify entities connected to networks, never people;
- IP addresses are frequently dynamically assigned by mechanisms such as Dynamic Host Control Protocol (DHCP) and hence do not have the stability required for personal identifiers.

Internet Protocol Version 6 (IPv6) is a new protocol that provides some significant enhancements to the existing IPv4 protocol. Enhancements that are of most relevance in the context of alternative personal identifiers are:

- a greatly increased addressing range that easily allows for an IP address for every individual on the planet plus one for all of their terminals;
- greater inbuilt security than IPv4 which is quite poor in the level of security provided.

IPv6 is unlikely to replace IPv4 in any short timescale and can be expected to co-exist with it, with tunnelling techniques being employed to interconnect "islands" of IPv6 implementation.

### C.1.2.2 Internet: DNS, URL and e-mail addresses

The entire Internet depends on an immense, distributed, globally trusted yet insecure naming service: the Domain Name System (DNS). DNS is the service that currently handles Internet names. It follows a design using a distributed database [11]. The system is designed to provide a quite simple but crucial operation: to handle a file of names and Internet addresses called hosts.txt.

There are several principles guiding its operation [11]:

- most of the data in the system are assumed to change very slowly (e.g. mailbox bindings, host addresses), but the system is designed to be able to deal with subsets that change more rapidly (on the order of seconds or minutes);
- access to information is more critical than instantaneous updates or guarantees of consistency;
- DNS is designed so that is backward compatible with networks or systems previous to the Internet as we know it, and is the result of many compromises to make the system more effective at the moment it was designed.

Another cornerstone of Internet naming and addressing is the Universal Resource Identifier, or URI. These are described in [12]: a Universal Resource Identifier (URI) is a member of this universal set of names in registered name spaces and addresses referring to registered protocols or name spaces.

Example 1: http://www.etsi.org/index.htm is a URI.

The well-known Uniform Resource Locator (URL) is a form of URI that expresses an address that maps onto an access algorithm using network protocols. Nowadays the standard protocol to access information in the Internet is http, and thus most of the URLs in common use begin with these four letters:

Example 2: http://www.etsi.org/index.htm is a URL

ftp://www.ucla.edu/index.htm is a URL

These identifiers often, but not always, contain quite meaningful information. They do, however, frequently change as people move or reorganize the structure of their WWW sites.

An identifier that may change frequently as people reorganize things behind it would not have the required stability for a Universal Communications Identifier. There is also a limit to the number of meaningful URLs that can be created and to attempt to identify a large number of people with them would not be practical.

The other cornerstone of the Internet is e-mail. Although a number of different forms of email have been implemented and although some, like X.400 [2] still remain, the predominant form of email today is Internet email. Internet E-mail addressing is handled as defined in RFC 822 [13]. The basis of the Internet e-mail system is the distribution of the naming mechanisms: In the case of formal registration, an organization implements a (distributed) data base which provides an address-to-route mapping service for addresses of the form:

person@registry.organization

A mechanism for accessing "organization" is universally available, the DNS. It is assumed that the system which operates under the name "organization" knows how to find a subordinate registry. The registry will then use the "person" string to determine where to send the mail specification. Once the network is accessed, it is expected that a message will go directly to the host and that the host will resolve the user name, placing the message in the user's mailbox.

For most people Internet Service Providers (ISPs) allocate their email addresses as a function of their names or roles. ISPs may be companies that provide Internet services to individual members of the public or they may be corporations that provide Internet services to their employees. Each ISP will have one (or more) internet domain names (e.g. "myprovider.com"), and the email addresses are formed by appending a name that is unique to that domain in front of the domain name and separated from it by an "@" (e.g. john.smith@myprovider.com).

In the example above, "john.smith" represents, by convention, someone with the name "John Smith". This name, however, could be an alias and not the email address owner's real name. Also, the receiver does not know whether "myprovider" is a public service provider or the company that John Smith works for. Additional security mechanisms, such as the use of certificates, at the client or server end of email systems can provide reliable originator information that basic Internet email lacks.

# C.2 Technical enhancements to basic schemes

## C.2.1 Supplementary services

The traditional approach to managing the linkage of a telephone number to a single telephone terminal in a telephony environment has been for the called person to subscribe to and activate various supplementary services. For example, when a person moves from their normal home terminal to a known distant terminal they can activate the Call Diversion supplementary service from their home terminal in order that they will be able to receive calls at the distant terminal. This approach places a heavy load on the user, in remembering to activate and, not least to deactivate the relevant supplementary services. These supplementary services have a very unfriendly underlying activation/deactivation protocol of star/square codes. It is also necessary for the user to select one or more of a basic set of simple supplementary services to achieve their mobility related aim. The supplementary services do not form a purpose designed mobility management interface and all of the work to maintain effective mobility management is placed on the user.

Calling Line Identity (CLI) and Calling Name Identity (CNI) services offer a means to present the identity of the calling party to the party being called. However, CLI is far more common than CNI and this only indicates the number of the calling line which, as stated in 1.1, does not identify a person or organization. The fact that for many network-to-network calls the CLI and CNI information is not passed between the networks means that in many cases CLI and CNI displays indicate that the information is not available.

Selective Barring Supplementary Services can be used to bar calls from a specified list of numbers or to bar all calls except those from a specified list of numbers. Unfortunately, the usefulness of these services is restricted by the fact that only telephone numbers can be listed whereas it is more likely that the intention is to bar calls from specified people or organizations not telephone lines. The firm link between users and telephone lines is decreasing rapidly as people become more mobile and have access to a greater number of terminals.

### C.2.2 Commercial 3rd party services

Commercial 3rd party services have evolved to try to ameliorate the limitations of the basic telephony service or any other service provided by multiple service providers. These services frequently package the functionality of traditional supplementary services with additional facilities such as call answering services. These services give users much greater control of their telephony environment, but the usefulness of these services is also restricted by the fact that telephone numbers give no direct indication of the identity of the caller. For example, if a call waiting service were to display the identity of a waiting call it could only say, "01473-223456 is trying to call you." which may well not tell you enough to identify the caller.

### C.2.3 Universal Personal Telecommunications (UPT)

Universal Personal Telecommunications (UPT) services allow users to be accessed by a common personal identifier (the UPT number) irrespective of what physical terminal they are connected to.

For the UPT subscriber to ensure that they are reached at a specific terminal they must employ one of at least two methods:

- the subscriber must dial an access code and then register their presence at the telephone terminal;
- the subscriber must insert a Smartcard into the telephone terminal.

The single UPT number can potentially overcome the problem for the caller when the party they wish to contact (the UPT Subscriber) frequently uses a multiplicity of different telephones and roams to completely new telephone terminals. However this number still does not contain any information that, to someone unfamiliar with the number, uniquely associates the number with the person to whom the number has been allocated. It does not therefore function as a very meaningful personal identifier. Also the system only works well where the UPT Subscriber successfully registers at every telephony terminal they may be using.

### C.2.4 Personal Numbering Schemes

Commercial Personal Numbering schemes adopt a variety of different approaches to allowing a single number to reach a party who is using a variety of different telephones. In addition, many of these schemes also incorporate a number of other value-added facilities such as call answering services. However, in principle most of them enjoy similar benefits and similar disadvantages to those described in clause C.2.3 for UPT systems.

## C.3 Users' strategies for managing their communications

The present document proposes a future environment in which users have a single Universal Communications Identifier which they give to those who wish to communicate with them and by which any or all of their terminals and services may be addressed. In contrast, in the present situation there are a range of different service and terminal specific identifiers which their owner may use to manage incoming communications or which a caller may use to manage the way in which their communication is presented.

This clause examines the ways in which users currently exploit this variety of identifiers in order to manage their communications. It is necessary to understand users' current strategies in order to ensure that the user requirements described in the present document reflect the need to give users a similar degree of control of the communications environment for both incoming and outgoing communications.

### C.3.1 Incoming

At present, users can exploit the range of different terminals and independent communication channels to manage their communication in a way that satisfies their needs. For example, a person can divert calls made to their home telephone number to their mobile telephone, which effectively makes their fixed telephone move with them on their travels. Similarly, people can avoid being disturbed by calls on any of their telephones by diverting all their calls to a single answering service. With email, the user may have an option to redirect email messages to a GSM mobile telephone as an SMS text message. This flexibility is currently obtained with some set-up difficulty for the user.

In an environment where a wide range of independently addressed terminals is replaced by one where the normal method of contacting a party is through a single Universal Communications Identifier, the party will need to be provided with facilities that give it the equivalent flexibility in call management.

## C.3.2 Outgoing

At present, users can exploit the fact that the party they are contacting may have a wide range of terminals with independent telephone numbers to help them achieve their communication needs. When communicationg with a 3$^{rd}$ party, some thought is usually given as to which telephone number should be used. Take the example of a user who wishes to give a message to someone in a different timezone who may well be asleep. In order to avoid waking them, the user may choose to phone their home telephone number rather than their mobile number if it is known that they always switch-on their answering machine at night. This, however, presumes extended detailed knowledge about the called party.

As with clause C.3.1, there is a need to replace the functionality that exists in the current environment with equivalent functionality when a wide range of known telephone numbers and email addresses is superseded by an environment where most people only know a single Universal Communications Identifier. It will be necessary to ensure that when initiating a communication the originator has the possibility to specify some special requirements. Whether the originator's requirements are satisfied depends on how conflicting originator and receiver requirements are resolved in establishing the communication.

# C.4 Mobility Management

## C.4.1 Mobility Management in telephony

In an environment where people are increasingly mobile and where they expect to be always able to contact others and to be contacted, three different approaches to managing mobility have emerged. These methods are described in the next two clauses.

### C.4.1.1 The mobile person controls their environment

One approach to mobility is to place the responsibility for controlling their availability on the roaming user taking some appropriate action. By the use of supplementary service, UPT systems, or Personal Numbering services, the user that roams should ensure that their communications environment is configured such that a caller will reach them at the terminal to which they currently have access.

### C.4.1.2 The system keeps track of the terminal

The GSM mobile environment represents an alternative approach to mobility management. This approach differs in that it is assumed that the terminal will be moving with the user and that it is likely that the terminal will be associated with a single person. The environment is able to automatically track the location of the terminal. This capability is extended to tracking the location of the terminal even when the user is roaming to a different country.

### C.4.1.3 Comprehensive mobility management

The above approaches both have their merits and future systems will adopt the basic functionality of both approaches to achieve the maximum flexibility in reaching the intended party.

## C.4.2 Mobility management in the Internet

A broader range of methods to support mobility management has evolved in the Internet. These methods include remote access log-ins to corporate mail servers, to Web based email management and roaming agreements between collaborating Internet Service Providers. With these methods the user may be able to have complete access to their full desktop environment, particularly when they carry their own laptop PC with them.

# C.5 Personal User Agents

In current and proposed architectures (Annexes C & D) there may be software entities that perform actions on behalf of those wishing to communicate. In the present document such an entity is frequently referred to as a Personal User Agent (PUA). The descriptor "agent" is chosen to show that it performs actions on behalf of (as an agent of) a user. The name does not imply any particular software architecture that may be associated with the name "agent".

Examples of such software entities are the software that keeps a record of the location of a user when they roam from place to place, the software that holds details of frequently called numbers, etc.

# C.6 Directories

Directories currently in use in the telephony and internet worlds suffer from one or more of the following limitations: they are proprietary, limited, or local and most attempts at some form of global directory are failures. In any scheme in which a global, cross-service communications identifier is used, there is a need for comprehensive and globally accessible directories. With the introduction of new universal identifiers there will be a need for a number of inter-linked directories that effectively form a single logical directory containing these identifiers. For role and person identifiers in a business environment there is a need for corporate directories that have selective public access for the public communications points within those organizations.

There is a longstanding and evolving body of experience and expertise associated with Directories. The X500 series of ITU-T Recommendations [3], [4], [5], [6] describe the essential features associated with directories. Much of the directories standards work is focussed on the issue of corporate rather than public directories.

A comprehensive system that allows the lookup of any Universal Communications Identifier is needed in any successful Personal Identification system. Fortunately, the concepts of Administrative Domains and Private Domains that are defined in the X.500 series Recommendations form a basis upon which such a comprehensive lookup system for public and private personal identifiers could be based. Issues of how this database could be populated and how appropriate privacy could be maintained would need further study.

# C.7 Real-time vs Store-and-Forward

The basic model for voice telephony is real-time communication. In the Internet, there are a variety of real-time voice and text "chat" systems, but perhaps the most popular communication mode is email, which is a "store-and-forward" (or perhaps more accurately "send-store-and-retrieve") mode. Different user identifier formats and protocols have evolved for these different modes of communication. An objective of any future Universal Communications Identifier is that they ought to be able to be used with all forms of electronic communication, both real-time and store-and-forward.

# C.8 Security/Privacy

Today's communications systems provide quite limited protection for many of the security/privacy threats outlined in Annex E. As well as concerns about the effectiveness of protection of the communication content, there are a number of weaknesses that relate to issues of the identification of the communicating parties.

There are opportunities for providing additional mechanisms to enhance the protection from these threats. Such mechanisms in use today include encrypting the information content of the communication and the provision of certification of the identities of the communicating parties.

# C.9 Terminals not people

Email Addresses, Personal Numbering and UPT are three approaches that give an identifier that relates to the party being called and not to the terminal. However, despite meeting this fundamental requirement of the Universal Communications Identifiers that are sought in the present document, each of these fails to provide an ideal solution on several other counts. The analysis of telephone numbers and email addresses in clauses 8.2 and 8.3 list many of these limitations.

# Annex D (informative): Emerging architectures

## D.1 3GPP

The 3rd Generation Partnership Project (3GPP) (www.3gpp.org) is an initiative taken by the partnership members to develop specifications for a number of releases of 3rd generation communications systems. The starting point for the work was to build upon many of the features of GSM. Features that have been taken as an essential element of 3GPP include the highly successful GSM concepts of the Subscriber Identity Module (SIM) and roaming. Both the SIM and roaming have many of the characteristics that are needed to achieve a successful personal identification system. The SIM already contains something close to a personal identity that can easily be associated with any compatible handset. The functionality behind roaming already uses many of the mechanisms that the Personal User Agents described in the present document would need in order to know the location of the person being contacted. Central to many of the 3GPP conceptual documents is the emphasis on identifying people rather than just with the identities of terminals.

A very similar initiative, based upon a different technical starting point, has been labelled 3GPP2. This too incorporates the same key concepts.

## D.2 TIPHON

The TIPHON project within ETSI defines an architecture for delivering a standardized system of telecommunications services over the Internet. The use of the Internet for the delivery of communications sessions makes an ideal platform in which personal identifiers can be used to help determine the most appropriate terminal identity for "terminating" the communications session.

## D.3 ITU SG13

ITU Study Group 13 has a question 29 on "Telecommunications architecture for an evolving environment". At least one proposal under discussion is for an "Information Communications Architecture (ICA)" (see annex G). This proposal hypothesizes an architecture with three agents - a "Contact Agent", an "Exchange Agent" and a "Transport Agent". The functionality of these agents provides intelligence that would enable very many of the requirements in the present document to be provided.

## D.4 The Internet

In addition, a number of IETF initiatives are related to the topic of user identification. The topics that are of most relevance are Universal Resource Identifiers (URIs), Universal Resource Names (URN), Common Name (CN) and ENUM. These are discussed in clauses 4.1, 4.2, 4.3 and 4.4 of this annex together with email addresses that are discussed in clause C.1.2.2.

### D.4.1 URI

Universal Resource Identifiers (URIs) (see annex G) are described as persistent location-independent identifiers for Internet resources. The URI is a more general form of the URL (clause C.1.2.2) and new types of URIs are regularly being proposed. Some of these may overcome some of the limitations currently found in URL's. However, all URIs still suffer from being related to Internet resources and not people.

## D.4.2 URN

URNs are defined in an Internet Request for Comment (see IETF/RFC 2396, annex G) as URIs that have a global scope and are globally unique. They are expected to persist and to be self-contained, scalable and extensible such that the range of URNs can always be added to. It is expected that resolution (i.e. translation) services will be available for converting the URN into something that directly points to an Internet resource e.g. a URL. Different URN namespaces can be defined to refer to different types of resources (from people to ISBN book references).

## D.4.3 Common Name

At present there are a number of proprietary systems that provide a way of associating an obvious and easy name with corporate WWW sites. The "Common Name" proposal from the IETF (see "Context and Goals for Common Name Resolution", annex G) is an attempt to define an open version of these schemes. The IETF "Common Name" has been proposed as a word or phrase, without imposed syntactic structure, which may be associated with a resource. Common Names are expected to be used primarily by humans (as opposed to machine agents). The IETF documents (see "Context and Goals for Common Name Resolution", annex G) indicate that they lack syntactic structure; there is no requirement of uniqueness or persistence of the association between a common name and a resource. The scope for conflict between names and the intellectual property rights relating to names are not addressed in (see "Context and Goals for Common Name Resolution", annex G).

## D.4.4 ENUM

The ENUM Internet draft (see annex G) defines a way in which E.164 numbers can be encoded so that the Internet Distinguished Name Service (DNS) can be used to route Internet telephony calls. It is proposed that the E.164 number is written backwards, with dots between groups of digits in the manner in which IP addresses are written. In this form, a standard DNS lookup method could be used to route the calls.

This method is still in an early stage of development and reservations have been expressed over whether the very large DNS tables that would be needed could be kept updated in a suitable timeframe to allow for the sort of terminal mobility that is accepted in the mobile telephony world. This method might be more appropriately used to locate software entities that control a user's communications (Personal User Agents) as it is expected that these would not need to move about but that they could remain on a server somewhere for significantly long periods of time.

# D.5 Implications

A common theme amongst all emerging architectures is the concept of a software entity or entities that manages the user's communications. In particular, this software entity needs to be aware of which terminals the user has access to, the probable location of the user, maintain communication histories, and take account of their communication needs. This software entity has been referred to in the present document as a "Personal User Agent" or "PUA".

Several of the emerging architectures assume that the identifiers that are used (be they E.164 numbers or Internet URIs) will be user identifiers rather than identifiers for terminals. This implies that the terminal may move with the user or that a user profile may be able to map the user to appropriate terminals. In cases where the identifiers no longer represent single terminals, the underlying systems must provide facilities that give originating users the same flexibility that they obtained from an understanding of which specific terminal they were trying to contact.

Current systems still provide the user with some information on the potential tariff of a communication based upon the identity of the number being contacted. Any future system is unlikely to be able to provide this potentially simple way of assessing communication costs and hence some alternative methods of providing tariff and cost information are likely to be provided.

Originating users are able to perform some communications management based upon the characteristics of the identifier being contacted. Where future systems are not able to guarantee such a predictable relationship between the characteristics of the identifier and the nature of the terminal, some alternative means of allowing originating and receiving users to mange their communicating strategies will need to be provided.

The priority assigned to a communication can also currently be inferred from characteristics of the number that is calling or being called. Where this changes, future systems will need to provide a facility to determine and to set the priority associated with a communication.

All of the above implications suggest the need for a number of additional user requirements that relate to the environment in which the Universal Communications Identifier operates.

# Annex E (informative): Security

This annex summarizes the major issues of security and privacy that are relevant to the present document.

# E.1 Security

Security is a property of systems that are protected, i.e. that minimize all types of vulnerabilities to their users, functions and resources. In our context, a vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security [4].

Security in this context refers to the problems that arise, for instance, when an unauthorized person gets information about a transaction or when someone masquerades as a legitimate user to get the credit card or other information.

There is an important distinction to be made between security and privacy. Privacy in this context refers to data protection against disclosure of data that the user wants to keep as private. Privacy is then a special function or property of a system, for which security measures have to be provided. E.g., who may have access to what information and what other uses of it are permitted? Privacy protection is becoming an important issue, as it is easier than ever to register user behaviour, the services are completely global, and this information can flow extremely quickly.

A key issue of a secure system is trust, which will only be achieved by providing both technological and legal solutions to increase the users' sense of security when using the telecommunications service.

On the technological side, the system can provide security procedures to reduce the risk of the different security threats identified. These technological protections have to be complemented by organizational measures, e.g., laws, "codes of conduct", and policies.

## E.1.1 Threats to security

It is convenient to present first the known threats to a data communication system regarding user identification (annex B of ITU-T Recommendations X.500 [3] and X.800 [7]).

1) **Identity Interception**

   The identity of one or more of the users involved in a communication is observed when the users involved do not wish so.

2) **Masquerade**

   A masquerade is where an entity pretends to be a different entity. A typical attack occurs when an authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges.

3) **Replay**

   A replay occurs when a message, or part of a message, is repeated to produce an 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).

4) **Traffic Analysis**

   The observation of information about a communication between users (e.g. absence/presence, frequency, direction, sequence, type, amount, etc.).

5) **Modification of messages**

   Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect, as when, for example, a message "Allow 'John Smith' to read confidential file 'Accounts'" is changed to "Allow 'Fred Brown' to read confidential file 'Accounts'".

6) **Repudiation**

The denial by a user of having participated in part or all of a communication.

7) **Denial of service**

Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions.

8) **Mis-routing**

The mis-routing of a communication path intended for one user to another.

# Annex F (informative): Background information

## 1. Background and policy documents

### 1.1 CEC Green Paper on a numbering policy for Telecommunications Services in Europe (Nov 96)

**Effective competition**

Carrier selection;

Number portability;

Restructuring of national numbering plans.

**Single Market**

Creation of a European Telephony Numbering Space;

Administration of European Numbering.

**Adapting to needs of Information Society**

Creation of long-term numbering plan for Europe;

Naming and addressing in the Internet and the other emerging multi-media and on line services (page 23).

### 1.2 ETSI GMM (Global Multimedia): Seamless Service Offering

Giving users consistent access to application/Service Portfolios independent of Access Network and Core Network (Jan 99)

**P30 – "Addressing Schemes**

**Access to called party by use of a single identity whilst:**

- Supporting existing addressing mechanisms (E.164 telephone number; X.121 address, X.400 [2] address; Internet address, etc.);
- Allowing various ways of addressing the individual if the preferred single identity is not known;
- Permitting different "single identities" for the same customer in a different environment (home/office, etc.);
- Avoiding "lock-in" of customers to a specific service provider;
- Avoiding the restrictions of the traditional numeric keypad.

- **Privacy**
  - Ensuring customers requirements for privacy are respected;
  - Providing for legal interception, means to over-ride policy, etc. in justified situations.
- **Emergency and assistance calls**
  - Provision of familiar and helpful procedures for emergencies, assistance and enquiries, irrespective of where in the world the customer is located.

### 1.3 CEN ISSS: Directory Workshop - X.500/LDAP Directories and High-level Naming (Web site)

A central point for telephony and Internet directory developments + links to other directory projects accessible on the net.

### 1.4 Internet Draft: URLs for Telephone Calls (Dec 99)

Under active discussion in the IETF. This is the definitive statement on how the Internet community currently see that telephone numbers can be represented as URLs in the Internet domain.

The document makes some extremely dangerous statements about how universally the E.164 number format is understood and supported in general usage (try putting an E.164 number in the "Telephone number" fields of many US Web sites to see how untrue that is!). They also suggest that strictly adhering to E.164 would make things easy for users - how many people in ETSI and the ITU know how to correctly write a number in the E.164 format - not sure if I do!

### 1.5 Other Internet Drafts

- E.164 number and DNS draft - technical issues of how Internet telephone numbers get handled + discussion of security, number portability, unified messaging (fixed mobile convergence?), etc.
- VPIM Directory - an internet directory document - full relevance not checked
- Voice Messaging Directory Service: Address Validation Schema and Message Routing Schema - full relevance not checked
- Voice Messaging Directory: Address Resolution Services - full relevance not checked

### 1.6 Draft report on Number Portability and its Implications for Tiphon Networks

Some issues related to portability, personal numbers and charging are included in the present document and should be looked at in more detail. TIPHON is, of course, ETSI's Internet telephony project.

## 2. Usability issues (including user requirements)

### 2.1 Jakob Nielsen's research: URL as UI (Jakob Nielsen - March 99)

- Good URLs
- Domain Names May Die
- New top-level domains is not a good way to go …"
- "The only top-level domain that is useful is .sex …."
- "New addressing schemes are likely to be introduced with better support for ambiguity and the ability to find things without knowing the exact spelling. Search engines and directories are an early attempt, but we can surely do better."

### 2.2 NetInvestigations.Net –Study of ideal email and web page addresses; a very brief experiment (Nov 99)

- Web page that show the experimental questions being asked by Helen Petrie at the University of Hertford, UK - a potential Workshop invitee.
- List and brief description of other studies including – Internet Addiction; Email diaries; etc.
- Summary of Internet Addiction study.

### 2.3 Future Computing Environments

The Web page of the FCE – "A group of students and researchers across various units at Georgia Tech who are interested in developing a culture and infrastructure on campus for the investigation, prototyping, and construction of computing environments now that we believe will be commonplace in 10-15 years time".

List of projects includes a look at user input error handling, ubiquitous audio and video, "The Context Toolkit", etc. Their "future project" "Cybernet" on "How we will provide mobile distributed network services in the future?" looks interesting and is linked to a DARPA project USAMAT: Unified Scalable Adaptive Mobile Application Toolkit" I think that this project also has funding from Motorola.

I think I have a project description bookmarked but not printed – its scope looks related to our work but its initial focus is more related to battlefield communications!

### 2.4 Mobile People Architecture (MPA) – Home Pages

Extracts from Web site

Person-level Routing in the Mobile People Architecture – the single most relevant paper (Nov 99)

User-Friendly Access Control for Public Network Ports – a technical description of parts of the infrastructure supporting MPA including a detailed assessment of some of the technical security issues.

### 2.5 Communication Patterns as Determinants of Organizational Identification in a Virtual Organization (June 98)

Academic paper that may have something to say that is of relevance to issues such as people's roles in organizations and how that affects their communications.

### 2.6 Re: Session-Id and privacy mechanisms (June 99)

Discussions the privacy issues associated with CallerID and how similar schemes for Internet CallerID should work. Who has a right to privacy and why questions.

# Annex G (informative): Bibliography

ITU-T Recommendation SG.13 D.735 (WP 1/13): "Proposal for an Information Communications Architecture (ICA)".

RFC 2972: "Context and Goals for Common Name Resolution", Nicolas Popp, Michael Mealling, Larry Masinter, Karen Sollins April 28, 2000 Expires in 6 months

Internet Draft draft-ietf-enum-rqmts-01.txt: "ENUM Requirements".

IETF (Internet Engineering Task Force) RFC 2396:"Uniform Resource Identifiers (URI): Generic Syntax", eds. T. Berners-Lee, R. Fielding, L. Masinter. August 1998

World Wide Web Consortium, "Recommendation: Namespaces in XML" http://www.w3.org/TR/REC-xml-names/, January 1999.

B. Anderson, et al: "Family life in the digital home - domestic telecommunications at the end of the 20th century", BT Technology Journal, Vol. 17, No 1, January 1999.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | January 2001 | Membership Approval Procedure MV 20010330: 2001-01-30 to 2001-03-30 |
| V1.1.1 | April 2001 | Publication |
| | | |
| | | |
| | | |