



***Feasibility Study of Personal User Agent and
Universal Communications Identifier
Technologies***

for

InternetNZ ENUM Task Force

by

Catalyst IT Limited

*Document version: 1.1
5 April 2005*

1 Opening Statement: ENUM Steering Group Chair



5 Enum is a service extension of the Domain Name System that links telephone numbers to Internet names and destinations. As Chairman of InternetNZ's Enum (e164.arpa) Task Force I welcome this report from Catalyst IT Limited. The report enables InternetNZ to advance plans for the implementation of Enum in New Zealand.

10 International trials of Enum Registry Services identified that critical to the real world success of Enum will be the security and privacy of individuals and organizations. To provide this support additional services such as UCI and PUA will need to be introduced which will protect end users from next-generation criminal threats as well as maximize the functional benefits of Enum to users.

15 InternetNZ tasked Catalyst with assessing the feasibility of enabling these services within the context of an Enum delivery service. Consumers, from professionals to parents, will read how Industry can support and protect them. The Telecommunications industry will see that UCI and PUA services enable them to offer their customers "new" services with positive revenue streams without attrition to current services. The Government will see that Enum consumer and commercial services can be implemented to protect citizens and national interest from the threat of spam, stalking and organized crime. Our society will therefore be able to maximize benefits from the full application of Next Generation integrated telecommunication services.

20 Catalyst's assessment provides a positive and constructive report based on international ITU and ETSI studies and it describes the operation of these services within New Zealand. InternetNZ will now discuss with stakeholders securing the resources necessary to commence implementation of a prototype for UCI and PUA services in support of Enum.

A handwritten signature in blue ink, appearing to read "Michael S. Sutton".

25

Michael S. Sutton
Chairman

InternetNZ - Enum Task Force

Phone: +64 4 472 1600 ext 730

30 **Email: michael.sutton@internetnz.net.nz**

2 Opening Statement: Catalyst IT Ltd



5 Catalyst IT are pleased to present this report evaluating the feasibility of implementing the infrastructure to move New Zealand's telephony into the age of IP networks, and outlining the steps to proceed along this road.

10 Our background in this area is in the creation and support of some of New Zealand's core Internet infrastructure, such as the root DNS servers and the Shared Registry System, and our role as IT providers for other identity-centric processes, such as New Zealand general elections, electoral rolls, and our role as an IT supplier for the Identity Services section of the Department of Internal Affairs.

The promise that the future holds is making communications between people as convenient and private as talking to someone you work next to, unconstrained by distance or their changing relationships with telecommunications providers.

15 ENUM, implemented with PUA and UCI technologies, can deliver that future.

A handwritten signature in black ink that reads "M. O'Connor".

Mike O'Connor

Director

Table of Contents

1	Opening Statement: ENUM Steering Group Chair.....	2
2	Opening Statement: Catalyst IT Ltd.....	3
3	Ownership.....	6
4	Definitions.....	6
5	Summary.....	7
6	Reasons to implement a PUA and UCI system.....	8
6.1	Are UCI and PUA needed to implement ENUM?.....	8
6.2	Relationship between ENUM, PUA, and UCI.....	8
6.3	Objectives of implementing a PUA and UCI system.....	9
7	How to implement and operate a PUA and UCI system.....	10
7.1	Allocation of ENUMs used with UCIs.....	10
7.2	Routing and access – the role of PUAs.....	10
7.2.1	Interfacing with a PUA.....	11
7.2.2	Commercial PUA provision.....	15
7.3	Requirements for PUAs.....	15
7.3.1	Clause 7.1 System capabilities related to input/output.....	15
7.3.2	Clause 7.2 System capabilities (internal/automated).....	16
7.3.3	Clause 7.2 System capabilities relating to UCI security.....	16
7.3.4	Clause 7.4 System capabilities relating to the UCI.....	17
7.3.5	Extended requirements.....	18
7.4	PUA development approach, including review of existing PUA software.....	19
7.5	UCI as identity.....	20
7.5.1	Types of identification.....	20
7.5.2	Registration processes.....	20
7.6	Risks of a PUA and UCI system.....	23
7.6.1	Eavesdropping.....	23
7.6.2	System component masquerading.....	23
7.6.3	Calling Party masquerading.....	24
7.6.4	Stalking.....	24
7.6.5	Denial of PUA service.....	24
7.6.6	Denial of Authentication Authority service.....	24
7.6.7	Denial of DNS service.....	24
7.6.8	Insecure final call connection methods.....	24
7.6.9	PUA design and configuration.....	25
7.6.10	Data assurance.....	25
7.7	Technical feasibility of PUAs and UCI.....	25
7.8	Conclusion and recommendations.....	26
7.8.1	Phase 1: prototyping and design.....	26
7.8.2	Phase 2: establish the infrastructure.....	26
7.8.3	Phase 3: involve the market.....	26
8	Conceptual system design.....	27

8.1	Conceptual entities.....	27
8.2	Examples of common transactions.....	28
8.2.1	Registration and allocation of a new number.....	28
8.2.2	Registration and conversion of an existing number to a UCI.....	29
8.2.3	Call from a UCI registrant to a normal telephony user.....	30
8.2.4	Call from one UCI user to another.....	31
8.2.5	Call from a PSTN Provider without an outbound PUA proxy to a UCI.....	32
8.2.6	Call from a PSTN Provider with an outbound PUA proxy to a UCI.....	33
9	Technical system description.....	34
9.1	Background – the technical architecture of ENUM.....	34
9.2	PUA and UCI software architecture.....	34
9.3	Use of SSL.....	35
9.4	System interfaces.....	35
9.4.1	Client device «» PUA.....	36
9.4.2	PUA «» PUA.....	37
9.4.3	PUA «» DNS.....	37
9.4.4	PUA «» Authentication Authority.....	38
9.5	Administration processes.....	38
9.5.1	Interception, search, and credential recovery.....	38
9.6	Operating a PUA server.....	38
10	Glossary.....	40
11	Document status and version history.....	40
12	Bibliography.....	41
13	Appendix: Terms of Reference.....	42

3 Ownership

This document is the property of Internet New Zealand. Internet New Zealand may release this document to the public, or to selected parties, at its discretion.

4 Definitions

5 A **Universal Communications Identifier (UCI)** record is defined¹ as:

- a numeric E164 format number
- an optional name
- an optional additional data field

An example of could be:

<i>E164 format number</i>	<i>Name</i>	<i>Additional Data</i>
+64 878 4803 2212	Mike O'Connor	CreateTimestamp=2005-02-08 14:22:11

10

The numeric component of a UCI can be used as an ordinary telephone number, but may support any form of communication. A UCI uniquely identifies a Called Party, regardless of location.

15 A **Personal User Agent (PUA)** is software that acts as a proxy for a user, negotiating the forms of communications to be used for outbound and inbound calls. A PUA can also decide not to allow communication to begin.

20 **ENUM** is an initiative that creates an area in the domain name system (DNS) that can be accessed by reformatting normal (E164 format) telephone numbers. ENUMs are specified to be country area code based (e.g. for New Zealand, the number starts with +64, and an example of a DNS entry is 2.1.2.2.3.0.8.4.8.7.8.4.6.e164.arpa). Querying an ENUM record returns a set of possible methods to establish communication. ENUM used in a PUA and UCI system would return just the URI for their associated PUA. We propose that the numeric component of a UCI is an ENUM.

25 Additional definitions may be found in the glossary, on page 40.

¹ ETSI EG 203 072 V1.1.1 Clause 5.1.1

5 Summary

5 PUA, UCI, and ENUM are key enabling technologies that will allow us to implement the successor to the current tangled network of cellphones, email, and fixed-line telephony. The key requirement is for each person to have a single number that defines their identity (a UCI), which stays within their control as they change locations, jobs, or service providers. ENUM provides the mechanism to store and access that number on the Internet, while PUA provides the tools needed to manage communications in an always-connected age.

10 Due to extensive work by the European Technical Standards Institute PUA and UCI are well specified, and for New Zealand's relatively simple requirements are sufficiently well developed to allow us to build upon them with confidence.

New Zealand's open and competitive telephone market will drive high-quality implementation of these services, and we expect that they will be taken up with gusto by the market as the benefits of focusing telephony on identity rather than location or carrier become clear.

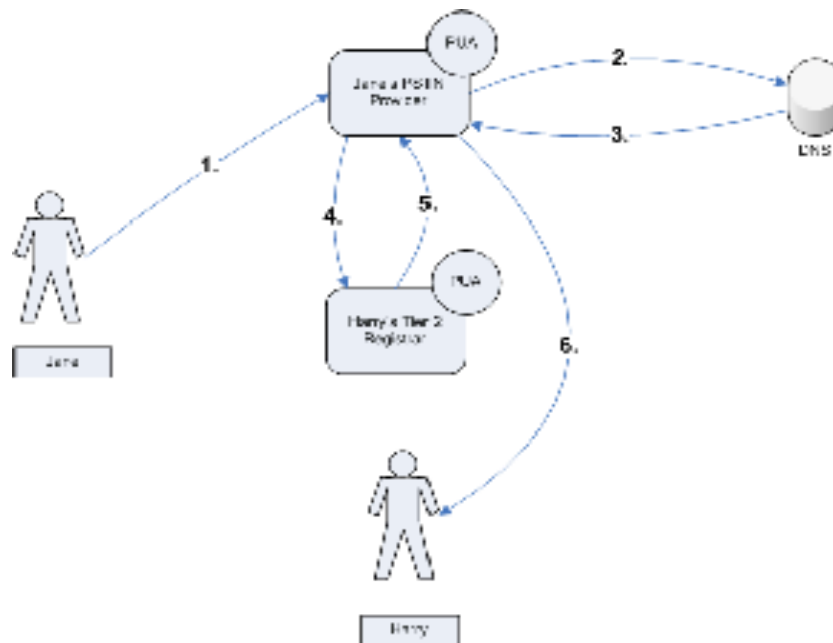
This paper recommends that:

- 15
- arrangements are put in place to allow allocation of telephone numbers for ENUMs
 - a prototype implementation of ENUM, PUA, and UCI be started
 - a formal design document be created that defines UCIs and outlines which areas of PUA development should be consistent and which left for the market to innovate
 - expressions of interest be sought to iteratively develop a working system, and

20

 - interested parties should be encouraged to develop commercial offerings based on PUA and UCI.

While implementing PUA and UCI would place New Zealand at the front of the field internationally, many of the components, such as ENUM, have been proven in trials. The system proposed will integrate well with European implementation of UCI and PUA when that occurs.



This diagram illustrates Jane calling Harry using an ordinary telephone, although Harry's phone is a VoIP phone that has a 802.11g connection to a wireless network.

6 Reasons to implement a PUA and UCI system

6.1 Are UCI and PUA needed to implement ENUM?

ENUM can be implemented without UCI or PUAs. However, ENUM without PUAs lacks privacy protections that would be essential for widespread adoption.

- 5 A UCI is a simple construct that allows a user's PUA to be identified. PUAs then have business rules that promote privacy. These can be divided into two categories: identity and control.

10 Identity business rules dictate that the normal mode of operation for a communication made using a UCI system is source authenticated. While registrants may initiate anonymous communications or communications using aliases, these will be clearly flagged, and we anticipate that client devices will warn about such communications.

15 Control business rules allow the user to specify what information is disclosed to who. It is our view that most users of UCI will not, in the medium term, wish to have unsolicited callers from outside their geographical region provided with personal information about them. The US-based ENUM Forum believe that the best approach to managing unsolicited communications (spam) is to introduce Federal and State laws. We disagree – we believe that infrastructure to make spam uneconomic needs to be planned into the implementation of ENUM. UCI and PUA are the best technology solutions to these problems..

6.2 Relationship between ENUM, PUA, and UCI

20 For the purposes of this review, the Terms of Reference (ToR) state how UCI and PUAs will relate to ENUM, and that UCI and ENUM in New Zealand will be provided together. Users will generally have a single UCI, but may have several ENUM. When a UCI is applied for, they will also have an ENUM allocated which matches the numeric component of the UCI.

To illustrate how the components of a future PUA and UCI system would fit together we introduce an imaginary user named Richard.

25 Richard works in Wellington, and has a pre-paid mobile phone and a traditional² phone. He then moves to Auckland, and buys a VoIP mobile phone. He applies for a UCI & PUA, requesting the number of the prepaid mobile phone he used in Wellington. He finds that he also needs to get a traditional phone to get Internet at home, so he uses that for some calls, and receives some on his VoIP phone.

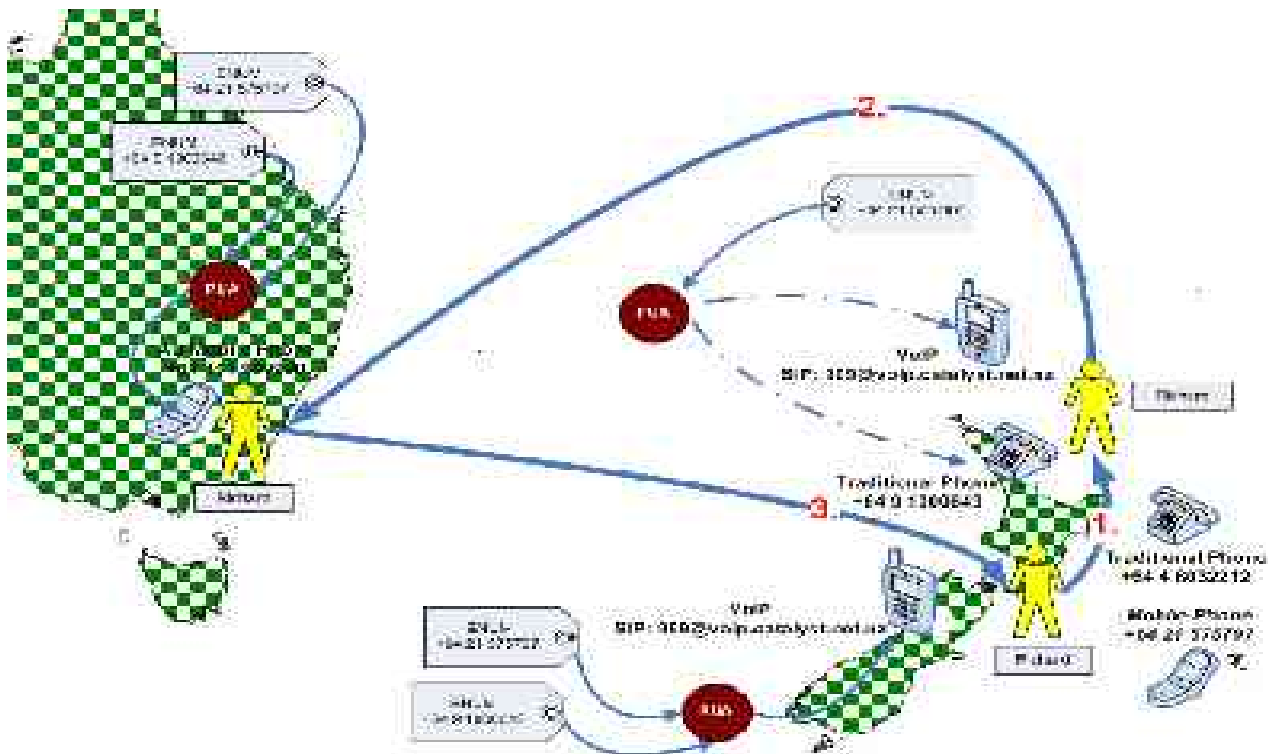
30 Shortly afterwards, Richard is offered a contract role in Sydney. Because people are used to calling him on both the ENUM that has been directed to his VoIP mobile phone and his Auckland phone line, he converts his Auckland phone number to another ENUM, which also points to the PUA associated with his UCI.

35 Once Richard gets to Sydney, he finds that his VoIP phone is incompatible with the local network. He gets his old cellphone he used to use back in Wellington sent over, and buys a local simcard, giving him an Australian mobile number. He sets up a simple profile on his PUA: route all incoming calls to his new mobile number, except at night, when it should send them all to answerphone. He doesn't disclose his new mobile number, reasoning that his two existing ENUMs are plenty.

2 PSTN

Once his contract role is over, Richard moves back to Wellington. This time he just needs to tell his PUA to send calls to his VoIP phone instead of to his Australian mobile, and his number doesn't change at all.

For a more detailed view of the components of the system, see *Conceptual System Design* below.



5 It should be noted that UCI is a proposal that has been largely defined by the European Telecommunications Standards Institute (ETSI). ETSI are still at a conceptual phase, and are not committed to the numeric component of a UCI being an ENUM – indeed, for them it is “[...] quite possible to envisage an implementation of UCI that is totally unrelated to ENUM.”³ This status does not reduce the benefits of using the UCI record structure in a New Zealand context.

10 6.3 Objectives of implementing a PUA and UCI system

The objective of implementing a PUA and UCI system is to enable the most appropriate form of communication in each circumstance, while still providing the convenience of traditional telephony. For example, a call to the normal UCI of a person who is currently using an Internet café in another country could be routed to the Internet access terminal that they are currently using. In comparison, under traditional telephony the likely outcome would be the Calling Party receiving an answering machine message informing them of (at best) the Called Party's mobile telephone number.

15 The effect of a well supported UCI and PUA system will be to commodify modes of transport for communications, and to seamlessly determine the optimum mode based on each party's preferences – for example, both may prefer least cost, in which case a low quality voice call might take place, or both may have subscriber-charged connections and support videoconferencing, in which case videoconferencing would take place.

Another objective is to allow appropriate controls to be placed upon communications. An example of this could be allowing parents to place controls upon PUAs used by children.

3 ETSI EG 203 072 V1.1.1 Annex D

7 How to implement and operate a PUA and UCI system

7.1 Allocation of ENUMs used with UCIs

5 The ETSI favour placing UCI numbers outside existing country codes. However, as ETSI UCI plans are not finalised, international numbers suitable for a PUA and UCI system are unlikely to be available in the medium term.

We recommend that numbers for UCIs be allocated from within New Zealand's country code, +64. In the long term, the ENUM entries associated with New Zealand UCIs can “point” to the same PUAs as UCIs within an international allocated numbering range, allowing a smooth future transition if international numbering is desirable in the future.

10 Given the infrastructure that will shortly be in place in New Zealand to support number portability, it is our view that the benefits of allowing an existing telephone number to be converted to an ENUM are greater than the benefits of being able to clearly identify that an ENUM number is not a conventional telephony number.⁴

15 As re-use of an existing telephone number will not be appropriate for all registrants, we recommend that a new number range under the +64 country code be allocated for new ENUMs, many of which will be associated with new UCIs.

20 In summary, we recommend that in the medium term numbers be allocated to support a PUA and UCI system under +64 from both existing geographical and cellular number ranges and from a new ENUM number range, while recognising that in the long term UCIs may be allocated at an international level.

7.2 Routing and access – the role of PUAs

The user of any conventional telephony device must be able to dial an ENUM associated with a UCI and receive a response. However, as few people wish to be available to all possible enquirers at all hours, that response may depend on a number of factors, including:

- 25
- the identity of the Calling Party
 - the local time for the Called Party
 - whether the Called Party is already engaged, e.g. on another call
 - whether the Called Party has scheduled non-availability (e.g. a meeting)
 - the location of the Called Party

30 In a typical example, if the Called Party is already on the telephone, options available to the Calling Party would be to continue the communication as an email or to leave a voice message.

35 Handling any case other than establishing a voice communication requires use of a PUA. Without PUAs, details of all possible means of reaching a Called Party would be publicly available⁵. This would be likely to result in the registrant being overwhelmed with unsolicited direct marketing (spam).

4 For counter-argument, see ETSI EG 203 072 V1.1.1 Clause 5.2.

5 See Assumptions of ToR

7.2.1 Interfacing with a PUA

A registrant's interactions with a PUA can be divided into two classes: those that require real-time interaction for a specific communication, and all other capabilities. This latter set are referred to as non-real-time interactions.

5 REAL-TIME INTERACTIONS

The below examples assume a terminal that supports video and voice or voice-only communication, where “dialtone” is a client interface to a PUA with a voice interface. The terminal is configured to use voice by default.

Example: real-time interaction with a PUA where location is requested

<i>Calling Party</i>	<i>PUA & System</i>
Enters a number to call Harry	
	PUA attempts to look up URI using DNS PUA retrieves URI for Harry's PUA Contacts Harry's PUA requesting a real-time voice call Harry's PUA requests the Calling Party's location to country precision PUA prompts “Country requested. Disclose? Please say 'Yes' or 'No'”
Says 'Yes' or 'No'	
	PUA passes location to Harry's PUA Harry's PUA responds by authorising the call, and supplying a URI for the voice call Call is initiated

10

Example: real-time interaction with a PUA where a preferred service is unavailable

<i>Calling Party</i>	<i>PUA & System</i>
Enters a number to call Jane	

<i>Calling Party</i>	<i>PUA & System</i>
	<p>PUA attempts to look up URI using DNS</p> <p>PUA retrieves URI for Jane's PUA</p> <p>PUA contacts Jane's PUA requesting a real-time voice call</p> <p>Jane's PUA responds that only video or text-based communications are supported</p> <p>PUA prompts "No voice calls allowed, sorry. To proceed, either say "Video" or end this call and send a text message. Video calls cost \$1 per minute."</p>
Says "Video"	
	<p>PUA contacts Jane's PUA requesting a real-time video call</p> <p>Jane's PUA responds by authorising the call and supplying a URI for the video call</p> <p>Call is initiated</p>

NON-REAL-TIME INTERACTIONS

15 A number of PUA capabilities are listed below that require registrant-PUA interaction. These are not initiated by a specific communication.

Example: Providing user profile status using a telephone

<i>Calling Party</i>	<i>PUA & System</i>
Dials a number for their PUA	
	PUA receives call, says "Please enter your PIN and then say 'Done' or press hash"
Enters PIN and says 'Done'	
	PUA says: "What do you want to do? Say 'List' for a list."
Says 'Describe Profile'	
	PUA says: "Accepted calls are sent to your mobile. Accept incoming calls from anyone in Address Book apart from Sam Fictus. Accept other incoming calls from New Zealand. Accept international calls except those marked as spam. To list rejected call rules, say 'Describe Reject Rules'"
Hangs up	

Example: Editing a user profile using the web

<i>Calling Party</i>	<i>PUA & System</i>
Using a web browser, selects the bookmark for their PUA login page	
	Requests a signed presentation of an SSL certificate from the client
Enters the passphrase for the SSL certificate loaded into their browser	
	Presents the PUA main page, including the following options: Manage destinations Manage incoming call rules Change spam detection settings Add a name to address book
Selects “Manage incoming call rules”	
	Presents a page that includes: Divert all calls to answerphone until (____)
Beside “Divert all calls to answerphone until”, enters “9am tomorrow” and clicks Apply	
	Presents a page allowing exceptions to be added, with an option called “Finish”
Selects Finish	
	Applies new rules and presents the PUA main page
Selects Logoff	
	Ends the session

Example: Searching the call log using a prepaid mobile telephone

<i>Calling Party</i>	<i>PUA & System</i>
Dials a number for their PUA	
	PUA receives call, says “Please enter your PIN, and then say 'Done' or press hash”
Enters PIN, and says 'Done'	
	PUA says: “What do you want to do? Say 'List' for a list.”
Says 'Search Calls'	
	PUA says: “Say 'To Name' or 'From Name'.”
Says 'To Robert'	
	PUA says: “The last call to Robert Smith was today at 9.25am. The calls before that were yesterday at 10.43pm, yesterday at 10.15pm...”

<i>Calling Party</i>	<i>PUA & System</i>
Hangs up.	

Example: Searching the UCI directory using the web

<i>Calling Party</i>	<i>PUA & System</i>
Using a web browser, selects the bookmark for their PUA login page	
	Requests a signed presentation of an SSL certificate from the client
Enters the passphrase for the SSL certificate loaded into their browser	
	Presents the PUA main page, including the following options: Manage destinations Manage incoming call rules Change spam detection settings Add a name to address book
Selects "Add a name to address book"	
	Presents a page that includes: Enter name Enter number Preferred type of call
Enters the name of the person they wish to add, and selects medium quality voice call	
	Requests a UCI directory list. Lists potential matches from the UCI directory, one of which has a green tick (note that this supposes the Authentication Authority querying each PUA after compiling the list, and a PUA may decline to answer)
Moves their mouse over the green tick	
	Displays a mouse-over message saying "This person has you in their address book"
Selects that person	
	Adds the UCI entry (comprising a number, a label, and a digital certificate) to the address book and presents the PUA main page
Selects Logoff	
	Ends the session

7.2.2 Commercial PUA provision

The provision of the PUA service will be crucial to the success of the PUA and UCI system. Typically, the PUA will be provided by an organisation that also provides Internet services, and accordingly has appropriate infrastructure in place, such as:

- 5 • billing
 - customer support
 - redundant power
 - secure environment for servers
 - redundant high-speed Internet connections
- 10 UCI registration will be sold by PUA providers, typically in a bundle with PUA services.

PUA providers will compete on:

- features
- price
- trustworthiness
- 15 • security
- user interfaces
- tie-in with existing services

For example, one PUA provider may offer a bundled UCI registration and PUA provision fee for \$100 per year, while another may offer greater services and guaranteed 99.9% availability and cost \$300 per year.

PUA providers will be required to support defined protocols, but will have freedom to develop their own user interfaces and client interaction strategies.

As the UCI itself is portable between providers, we expect that some customers will change providers several times, seeking the best combination of price, features, and non-functional attributes. However, most customers are likely to form a long-term relationship with one provider.

7.3 Requirements for PUAs

Requirements for PUAs are well specified in the document ETSI EG 202 067. Clause 7 of this document is generally appropriate for a New Zealand context. We have listed each requirement below, and allocated a priority of Mandatory, Important, or Optional. Mandatory indicates that the service should not be used without this capability. Important indicates that the absence of the capability would handicap the service.

7.3.1 Clause 7.1 System capabilities related to input/output

Providing user profile status (SC 1.1)	Mandatory
Editing the user profile (SC 1.2)	Mandatory
Selecting communication medium and characteristics (SC 1.6)	Mandatory
Access to personalised list of known UCIs (SC 1.4)	Important

Providing cost information (SC 1.7)	Important
Provide originator anonymity (SC 1.9)	Important
Identifying the originator of communication (SC 1.11)	Important
Users identifying themselves (SC 1.13)	Important
Awareness of cost implications of filtering/routing (SC 1.14)	Important
Availability of communication records (SC 1.3)	Optional
Determining a UCI (if unknown) by means of a search process (SC 1.5)	Optional
Assign priority to communication when necessary (SC 1.8)	Optional
Using an alias (SC 1.10)	Optional
Verifying the identity of the originator/recipient (SC 1.12)	Optional
User control of personal user agent (SC 1.15)	Optional

7.3.2 Clause 7.2 System capabilities (internal/automated)

User availability for communications (SC 2.2)	Mandatory (for a minimum subset)
Establishing contact where possible (SC 2.3)	Mandatory
Taking account of local time (SC 2.4)	Important
Barring/enabling incoming communications from specified originators (SC 2.8)	Important
Maintaining the functionality of network-specific services (SC 2.9)	Important
User location monitoring (SC 2.1)	Optional
Using the originator's alphabet (SC 2.5)	Optional
Using the user's preferred language for network information/instructions (SC 2.6)	Optional
Establishing the communication in a mutually acceptable language (SC 2.7)	Optional

7.3.3 Clause 7.2 System capabilities relating to UCI security

Provision/non-provision of location information (SC 3.1)	Mandatory relative to SC 2.1; otherwise Optional
Providing confidentiality/privacy of stored data (SC 3.3)	Mandatory
Provision/non-provision of availability information (SC 3.2)	Important
Providing confidentiality/privacy of communications (SC 3.4)	Important
Assuring identity (SC 3.3)	Important
Providing integrity (SC 3.6)	Important
Providing a non-repudiation capability (SC 3.7)	Optional

7.3.4 Clause 7.4 System capabilities relating to the UCI

Delivery and interpretation of a numeric part of UCI (SC 4.2)	Mandatory
Delivery (and possible processing) of a user friendly label to the recipient's PUA and terminal (SC 4.1)	Important
Delivery and processing of additional information to the recipient's terminal (SC 4.3)	Important

7.3.5 Extended requirements

SPAM FILTERING

5 A range of anti-spam measures need to be implemented with Important priority. The objective of any spam-control system must be to make large-scale unsolicited communications over the UCI and PUA system uneconomic.

10 As noted above, the US-based ENUM Forum is of the view that spam can be addressed through Government action. Their strategy for ensuring privacy beyond this is to provide no link between the E164 format number and the individual identity – by, for example, ensuring that names do not appear in URIs. It is our view this is unworkable – it would, for example, require non-meaningful email aliases to be set up to avoid use of a person's normal email address.

By contrast, the strategy that UCI provides is to ensure that communications are routed initially through a PUA, and provide sessions based on PUA-PUA negotiation that (where possible) authorise only a single connection. Other privacy strategies are discussed in ETSI TR 103 077 Clause 10, including limiting UCI disclosure and complex PUA behaviour.

15 Spam has not been a significant problem on the New Zealand telephony system to date, for the primary reason that per-call costs are high. However, the issue has grown to prominence due to the growth of spam using email as a transport. Most email traffic globally is now spam.

20 We believe that it is reasonable to expect UCI to UCI communications over commonly available transports to have a near-zero marginal cost, in the range of zero to five cents NZD per minute. While this low marginal cost has clear benefits, one disadvantage is the proliferation of spam. Spam has been shown to arise in any environment where the costs of attempting unsolicited communications are outweighed by the benefits – such as in the case of email, where the marginal cost per email is below one cent NZD.

An initial approach to spam reduction (assuming various non-mandatory capabilities) could be:

- 25
- If the Calling Party's identity is verified and the Calling Party is in the PUA address book, accept.
 - If the call is non-UCI, and CLI information is provided, and the call originates within New Zealand, accept.
 - Otherwise, identify as possible spam.
 - After the call is complete, allow user to add this UCI to a list from which calls are always either
- 30 accepted or rejected

A communication treated as possible spam could offer the Calling Party the option of continuing for a configured price, e.g. 30 cents NZD. This would have the benefit of providing callers who do not meet a registrant's criteria for *prima facie* trustworthiness to continue the communication, while providing a strong deterrent for someone initiating thousands of communications or more.

35 Another option presented by the ETSI is to allow a Calling Party who cannot initiate a call to leave their UCI details, without a message. This is compared to the historical practice of visitors giving calling cards to footmen.

Users must be able to configure, and if they desire disable, their spam filtering settings.

40 These are merely examples of spam control approaches, and undoubtedly many other solutions exist. Users could potentially choose between competing spam control options.

CHARGING

The spam control method discussed above requires charging to be supported at a PUA negotiation level. This is an additional requirement.

5 7.4 PUA development approach, including review of existing PUA software

For PUAs to be implemented at a useful scale, given the requirement for reliable network connectivity, server-side software will be needed.

10 After examining a range of software, we have concluded that while software exists that fulfils some requirements of PUAs, the most effective way to meet the requirements for PUAs would be through bespoke development rather than modifying an existing product. We identify a development strategy for such software in *Conclusion and recommendations* below. This development would use existing components wherever possible, which might, for example, involve re-using or extending Jabber interfaces or XML parsing code.

15 A question specifically asked in the ToR is whether it would be possible to build PUAs onto existing DNS server software. As a matter of principle, we feel that as PUAs and DNS provide different functions they should be independent. There are also practical problems with modifying DNS software to perform this role, as the tasks performed are quite dissimilar.

Some products that meets some subset of the requirements for PUAs are:

Microsoft Exchange Developed by Microsoft, Exchange is primarily a mail server. It supports out of office replies, routing of a number of different kinds of messages, and servers that understand communications in a range of formats.

SIP Express Router SIP Express Router is modular, and the following modules are available: accounting, digest authentication, CPL scripts, ENUM support, instant messaging, MySQL support, PostgreSQL support, a presence agent, radius authentication and accounting, diameter authentication, record routing, an SMS gateway, a Jabber gateway, NAT traversal support transaction module, a registrar, and user location.

Vocp Vocp is a messaging solution for voice modems, with voicemail, fax, email pager, DTMF command shell and Text-to-Speech support, 4 graphical interfaces, and a Web interface. Callers navigate the system using a touch-tone phone and may send and receive faxes, voice mail, and pager messages, listen to text/HTML email messages, or execute configured programs on the host and hear the resulting output.

AOL Instant Messenger AOL Instant Messenger supports Video Chat, Voice Chat, Messaging, and integration with external directories.

Jabber A streaming XML technology mainly used for instant messaging.

20 This is an incomplete review of software that meets some PUA requirements, and does not involve product evaluation. Fully reviewing software that meets the requirements identified is beyond the resources allocated to this review.

7.5 UCI as identity

A PUA and UCI system can provide the identity of the Calling Party to the Called Party, and quantify the strength of the identification process.

7.5.1 Types of identification

5 The following levels of identification have been identified:

- External Alias
- Legacy CLI
- Anonymous
- Alias (likely to be non-authoritative)
- 10 • Identified
- Identity Verified

External Alias would be any unverified label from outside the system, such as an email From: header. This could be null, the lowest possible form of authentication.

15 **Legacy CLI** identification would involve displaying either the number, or the name in a local address book associated with the number, that is provided by a legacy telephony system. This is a weak level of assurance, and only identifies the calling device being used, not its user.

Anonymous identification indicates that the call comes from a UCI device, but that the Calling Party has chosen to suppress their identity.

20 **Alias** indicates that the call comes from a UCI device, but that the Calling Party is not using their recorded name.

Identified means that the Calling Party's recorded name is displayed.

25 **Identity Verified** means that the Calling Party has been identified with a level of assurance sufficient for significant financial matters, such as providing access to telephone or Internet banking. In practical terms this would be likely to mean that the Calling Party, already Identified, was prompted for a shared secret before a communication.

7.5.2 Registration processes

Registration processes will determine the strength of the **Identified** and **Identity Verified** statement of identity.

The following information would be requested from a registrant:

- 30 • Surname
- First names
- Sex
- Date of birth
- Contact details
- 35 • (optionally) Telephone account details, or other evidence of identity

The registrant would also be required to select preference information, such as whether they want their UCI to be in the Authentication Authority's public directory.

Provision of this information would allow verification of name, and would allow selective release of (unverified) sex and age information.

- 5 Once all required information was provided to the Authentication Authority by the registrant's selected Tier 2 Registrar, the Authentication Authority would:
- Check that the application met established criteria, such as completeness and minimum age
 - (optionally) Verify that the person is authorised to make changes to the telephone account listed
 - Generate a token creating the UCI and authorising SRS to allocate it
- 10 Possible methods to establish identity are discussed below.

RE-USE TELEPHONE COMPANY IDENTIFICATION

One approach to registration is to take advantage of an already-authenticated service. One source that can be used to validate identity are telephone company records.

- 15 For those applying to convert an existing number to an UCI or ENUM, the telephone company confirmation that the registrant is authorised to change the number provides some validation of identity, although only to the weakest degree that the telephone company has historically sought proof of identity for new or changed account holders.

This form of identification would only be possible for those who are the account-holder for a contract mobile phone or fixed phone line, and would not require supplying additional data.

20 RE-USE BANK IDENTIFICATION

Bank accounts would be the preferred already-authenticated service for establishing identity. Bank accounts are particularly suitable for use as the bank is required to verify the identity of their holders by the Financial Transactions Reporting Act 1996.

- 25 An existing process to match information provided is a Direct Debit Authority, as this authority will only be loaded by a bank if the details on it match the details they hold and have previously verified. While clearly this would have potential synergies with charging, there is no necessity for the debit authority to ever be used once loaded.

This form of identification would require the following additional information:

- 30
- Name of bank
 - Branch
 - Account number
 - Signature

PRESENTATION IN PERSON TO AGENT, SUCH AS A POSTSHOP

- 35 The most rigorous form of identity checking is presentation in person, with a strongly authenticated identity document. Drivers license, passport, or other identity documents could be used. As there is

no mandatory photo identification in New Zealand, at this level of authentication some people would be unable to register.

The Authentication Authority could appoint an agent, such as New Zealand Post's PostShop network, to verify identity.

5 The process would be:

- registrant would apply to their Tier 2 registrar in the ordinary way
 - once the Authentication Authority received the application, they would generate a record for the agent stating the details of the registrant, and contact the registrant advising them of a token
 - the registrant would present in person to an agency, such as a PostShop, where the staff would enter the token provided and check that the registrant's face and signature matched the details on a form of ID
- 10

Only the final approach would have the benefit of allowing age to be verified as part of UCI identity. It is our view that the additional cost to registrants is not justified by this benefit.

7.6 Risks of a PUA and UCI system

The following usage risks have been identified:

- Eavesdropping
- System component masquerading
- 5 • Calling Party masquerading
- Stalking
- Denial of PUA service
- Denial of Authentication Authority service
- Denial of DNS service
- 10 • Insecure final call connection methods
- PUA design and configuration
- Data assurance

Project risks would also apply to the development.

7.6.1 Eavesdropping

- 15 The risk of call monitoring through the system proposed is that of the underlying call placing technology used after negotiation, plus the risk of a man-in-the-middle attack.

Because SSL is proposed, before compromise could occur:

- the SSL protocol would have to be compromised, or
- the PUA host would have to be compromised, or
- 20 • both the DNS and the Authentication Authority would have to be compromised.

It is our view that the risk of the latter attack vector being successfully exploited are low. The security of a PUA will be part of the selling points of each PUA provider, but is a weak point in the structure. The SSL protocols themselves are well reviewed, but vulnerabilities may emerge that require software upgrades.

- 25 We believe that the structure proposed would be likely to make physical monitoring less costly than system compromise.

7.6.2 System component masquerading

Masquerading is a possible risk for any entity in the system.

At a client to PUA level the difficulty of masquerading will depend on the connection method used.

- 30 At a PUA to PUA level masquerading will be difficult due to the SSL mechanism proposed.

DNSsec is a technical assumption of the system listed in the ToR, and is an important security improvement over currently deployed DNS.

Initial implementations of PUAs are likely to rely on CLI for at least one element of caller identification. While a full risk assessment of CLI masquerading is outside the scope of this paper, it should be noted that CLI is a risk point, and the implementers of PUAs should consider that when designing PUA security.

- 5 Masquerading of the Authentication Authority is a minor risk, as all parties will have a public key for them.

7.6.3 Calling Party masquerading

10 The risk of Calling Party masquerading is substantially lower than in the current PSTN system. Called Parties can choose to accept only identity verified calls, and will be warned if aliases are used. In the short to medium term, the primary risk will come from calls originating in the PSTN.

7.6.4 Stalking

15 The privacy protections built into PUAs will assist those at risk of stalking. These people will have to use white lists of Calling Parties who may communicate with them if they distribute their UCI, which will reduce usability for them. Blacklisting and judicious use of anti-spam settings will assist those in a more moderate risk category.

7.6.5 Denial of PUA service

20 Denial of the PUA service will have a major impact on the users of the PUA and UCI system. Service guarantees will be a major selling point of the PUA provider's service offering. The SSL architecture proposed somewhat increases the risk of denial of service attacks relative to a trusted peers structure.

7.6.6 Denial of Authentication Authority service

25 Denial of the Authentication Authority service will have a relatively minor impact on users of the PUA and UCI system, provided that non-response to OCSP queries is treated as success. If OCSP query non-response is treated as failure, then all communications between PUAs will halt if the Authentication Authority service is denied. For this reason it is recommended that non-response to OCSP queries is treated as success, but with a warning to the client.

7.6.7 Denial of DNS service

30 The DNS is a crucial element of the PUA and UCI system. If the DNS is unavailable, the system will cease operating. The DNS is, however, a distributed system with a strong track record of reliability.

7.6.8 Insecure final call connection methods

35 The PUA and UCI system specified does not deal with the final call connection between clients. These connections will use diverse technologies, and there is no guarantee that they will have encryption and masquerading protection built in. To mitigate this risk, the PUA would notify clients that supported it when they should expect a connection, and from which source.

7.6.9 PUA design and configuration

5 It is widely understood within information systems design that a system is as secure as its weakest component. With this in mind, PUA design will need to focus on ensuring that authentication and validation of inputs are applied to a consistent standard on all interfaces. As an example, there is little point in requiring all clients using PUAs to have client-side SSL certificates if the same clients could access the PUA by using a username and four digit PIN.

10 Security is also dependent on users perceiving value in it. Most users will not choose authentication methods that require per-use authentication to make a call, and as a result these PUAs will be subject to hijack and can potentially be used by parties other than the owner of the UCI. The technical architecture proposed will usually make PSTN the most effective route for compromise.

7.6.10 Data assurance

15 PUAs will disclose data, such as location, which from the point of view of the sending PUA will be correct. However, these PUAs will depend on insecure client devices to provide much of this information. As a result, PUAs will send incorrect data from time to time, either due to client device misconfiguration or deliberate injection of false data.

CLI and location are data particularly subject to corruption, and this should be taken into consideration when designing PUAs.

7.7 Technical feasibility of PUAs and UCI

In summary, PUAs and UCI are both technically feasible.

20 PUAs have well-defined requirements, and require always-on network connectivity. Existing software exhibits some of the attributes sought from PUAs, but overall the most effective approach would be to implement the software as a bespoke development, which would make use of publicly available standards and components.

25 There would be considerable benefit in a reference implementation of PUA software being available under an OSI-approved license⁶– this would promote innovation and interoperability.

To deliver UCI the required infrastructural components are PUA and ENUM. ENUM has been demonstrated to be sufficiently developed to return a URI for a PUA, although the standards around URI retrieval and formatting require specification.

⁶ <http://www.opensource.org/docs/definition.php>

7.8 Conclusion and recommendations

This conclusion and recommendation uses terms from the conceptual system design.

If InternetNZ wish to implement a PUA and UCI system, the process that we recommend would be the following phased approach.

5 7.8.1 Phase 1: prototyping and design

- Create a prototype implementation of ENUM, PUA, and UCI. This would demonstrate the primary functional elements of the system, but in a lightweight architecture and possibly without sufficient usability, reliability, performance, scalability, or security for a production deployment.
- 10 • Based on information gained from the pilot, produce a formal requirements document for UCI and for a minimalist PUA. We anticipate that this would largely confirm the ETSI requirements.
- Produce a formal technical design document for UCI and for a minimalist PUA, which clearly defines how additional PUA features and human interfaces can be added.

7.8.2 Phase 2: establish the infrastructure

- 15 • Encourage the development of gateway providers who can provide PUA of last resort services for legacy calls and provide PSTN to VoIP telephony translation
- Seek expressions of interest to develop a PUA and UCI system, using an iterative development process that first creates infrastructure and demonstrates end-to-end communication, without substantial functional elements (a proof of concept), and then proceeds to full development.

7.8.3 Phase 3: involve the market

- 20 • Once the development of the PUA and UCI infrastructure reaches an early testing stage, involve interested parties in constructing PUA extensions and interfaces to provide a marketable “look and feel”.

8 Conceptual system design

8.1 Conceptual entities

The conceptual system design is based on the assumptions in the ToR.

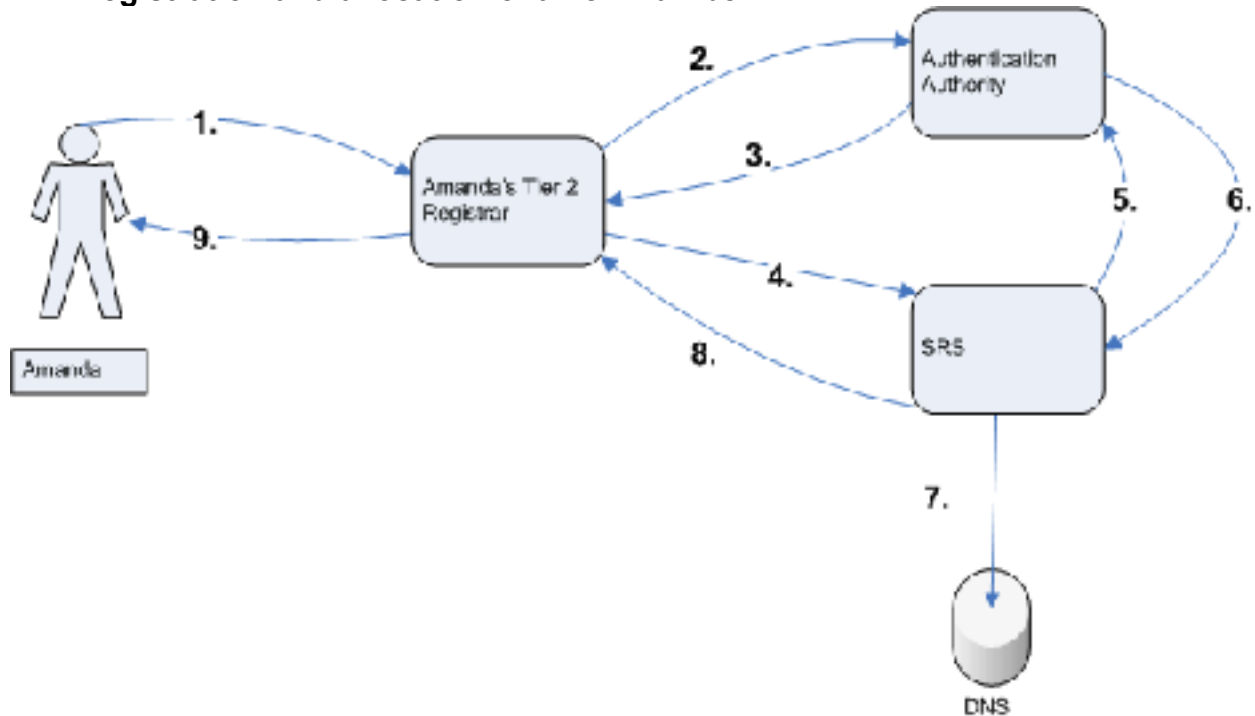
The system will have the following entities:

- 5 • **Tier 1 Registry**, which will be operated by InternetNZ or delegated agency. The Tier 1 Registry will be the delegatee for New Zealand ENUMs, i.e. 4.6.e164.arpa.
- An **Authentication Authority (AA)**, which will be operated by InternetNZ or delegated agency. This will verify identities; interoperate with telephone companies; maintain a directory of UCIs; and be the delegatee for the dedicated domain for ENUMs, such as 8.7.8.4.6.e164.arpa,
10 equivalent to +64 878 xxxx xxxx
- An **Appeal Authority** to hear UCI applications rejected by the AA
- A **Shared Registry System (SRS)** which contains ENUMs and UCIs, to which institutional actors will have access, and which has the **DNS** as a public view
- **Tier 2 Registrars (Registrar)**, which will operate PUAs
- 15 • **Registrants**, who are the end users of the system
- **PSTN Providers**, who are the incumbent telephony (PSTN) operators
- A **Gateway Provider**, which will provide a PUA and a PSTN to VoIP gateway of last resort where the Calling Party's PSTN Provider does not provide them
- **PUAs.**

20

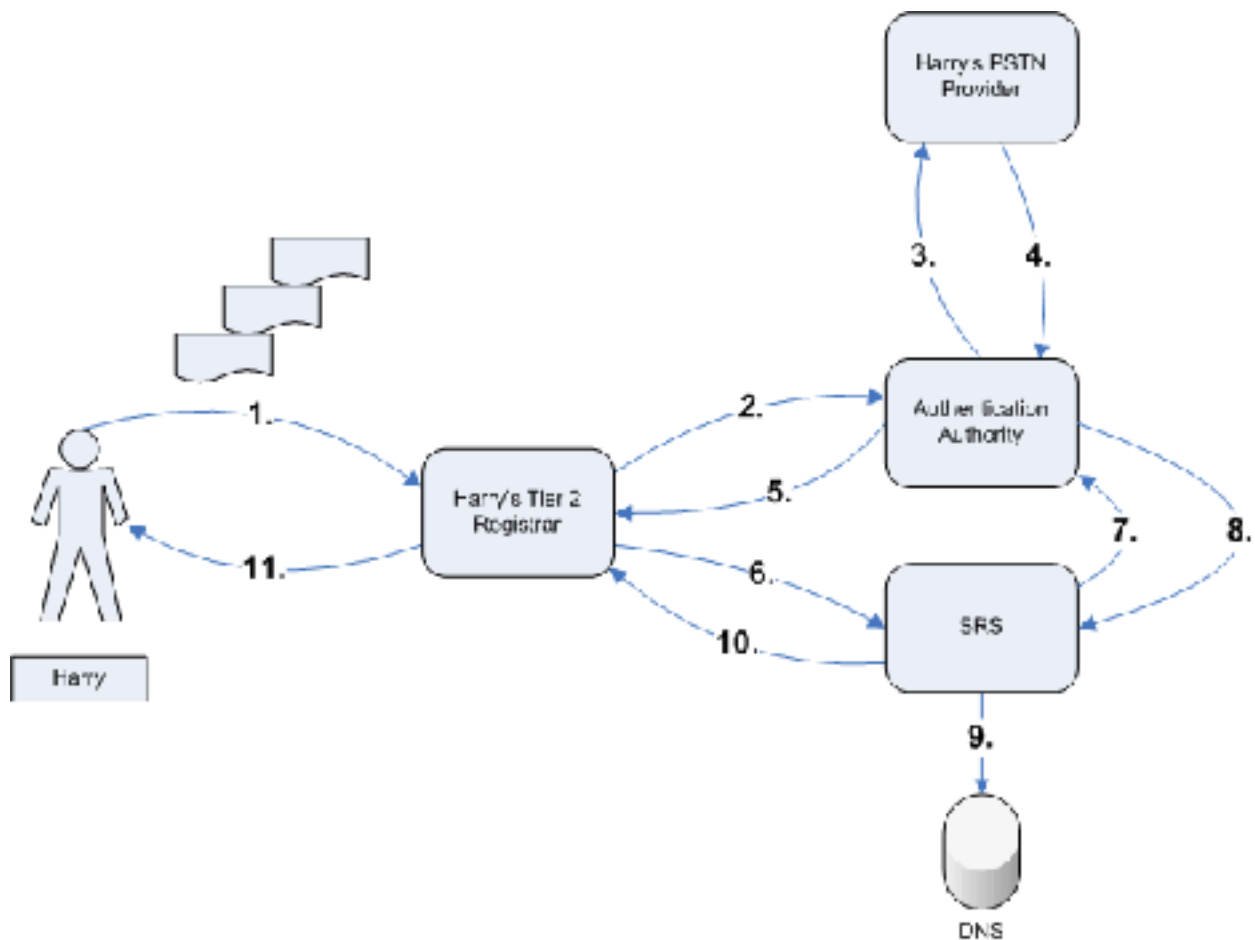
8.2 Examples of common transactions

8.2.1 Registration and allocation of a new number



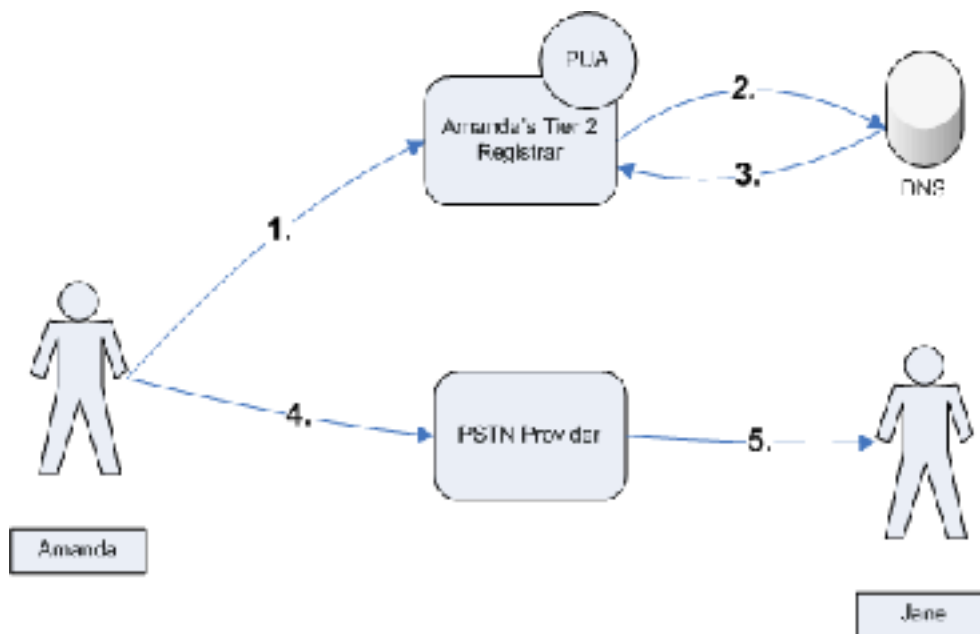
- 5 1. Amanda, the registrant, provides evidence of her identity to her chosen Registrar
2. The Registrar applies on her behalf to the AA
3. The AA approves the application and supplies a token
4. The Registrar enters these details into the SRS
5. The SRS passes the token to the AA for validation
- 10 6. The AA creates a UCI and replies that the token is valid
7. The SRS adds the matching ENUM record into the DNS
8. The SRS provides the UCI to the Registrar
9. The Registrar notifies Amanda of her new UCI and provides information on how to use it

8.2.2 Registration and conversion of an existing number to a UCI



1. Harry, the registrant, provides evidence of his identity to his chosen Registrar, including the number he wishes to register and a copy of a recent telephone bill
2. The Registrar applies on his behalf to the AA
3. The AA asks Harry's PSTN Provider if Harry is authorised to change this number, and notifies them that the number is changing to an ENUM
4. Harry's PSTN Provider replies that Harry is authorised and Harry's details are correct
5. The AA approves the application and supplies a token
6. The Registrar enters these details into the SRS
7. The SRS passes the token to the AA for validation
8. The AA creates a UCI and replies that the token is valid
9. The SRS adds the matching ENUM record into the DNS
10. The SRS provides the UCI to the Registrar
11. The Registrar notifies Harry of his new UCI and provides information on how to use it

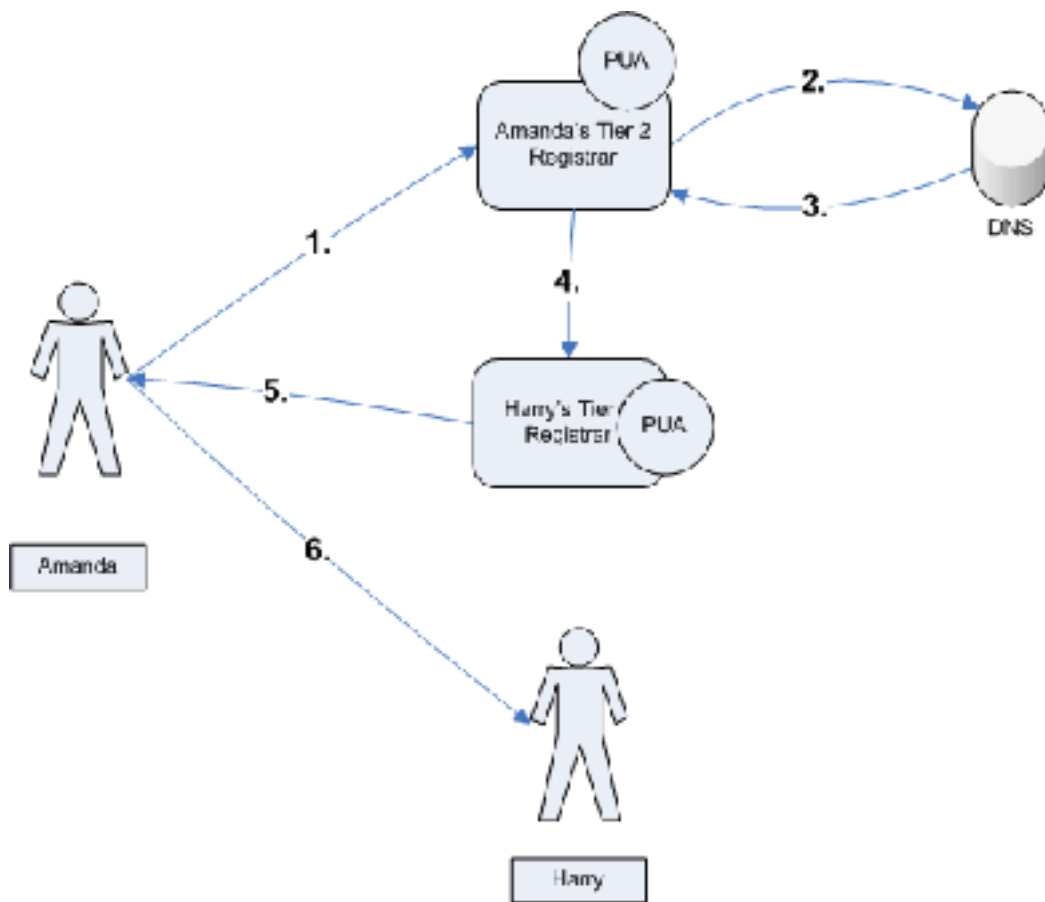
8.2.3 Call from a UCI registrant to a normal telephony user



Preconditions: Amanda has registered with her PUA.

- 5 1. Amanda, the Calling Party, selects Jane's name from her address book and initiates a voice call
2. Amanda's PUA looks up the e164.arpa namespace for the supplied number in the DNS
3. The DNS replies that the number is not known
4. Amanda's terminal places a PSTN call to the number provided
5. Jane receives the call

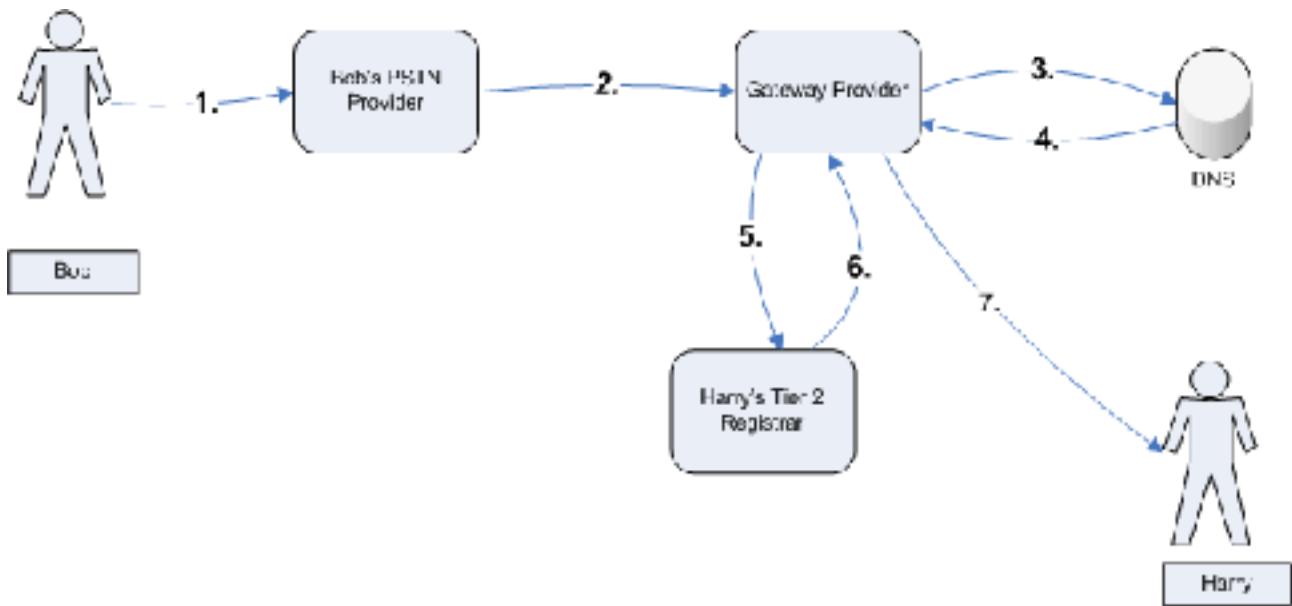
8.2.4 Call from one UCI user to another



Preconditions: Amanda has registered with her PUA.

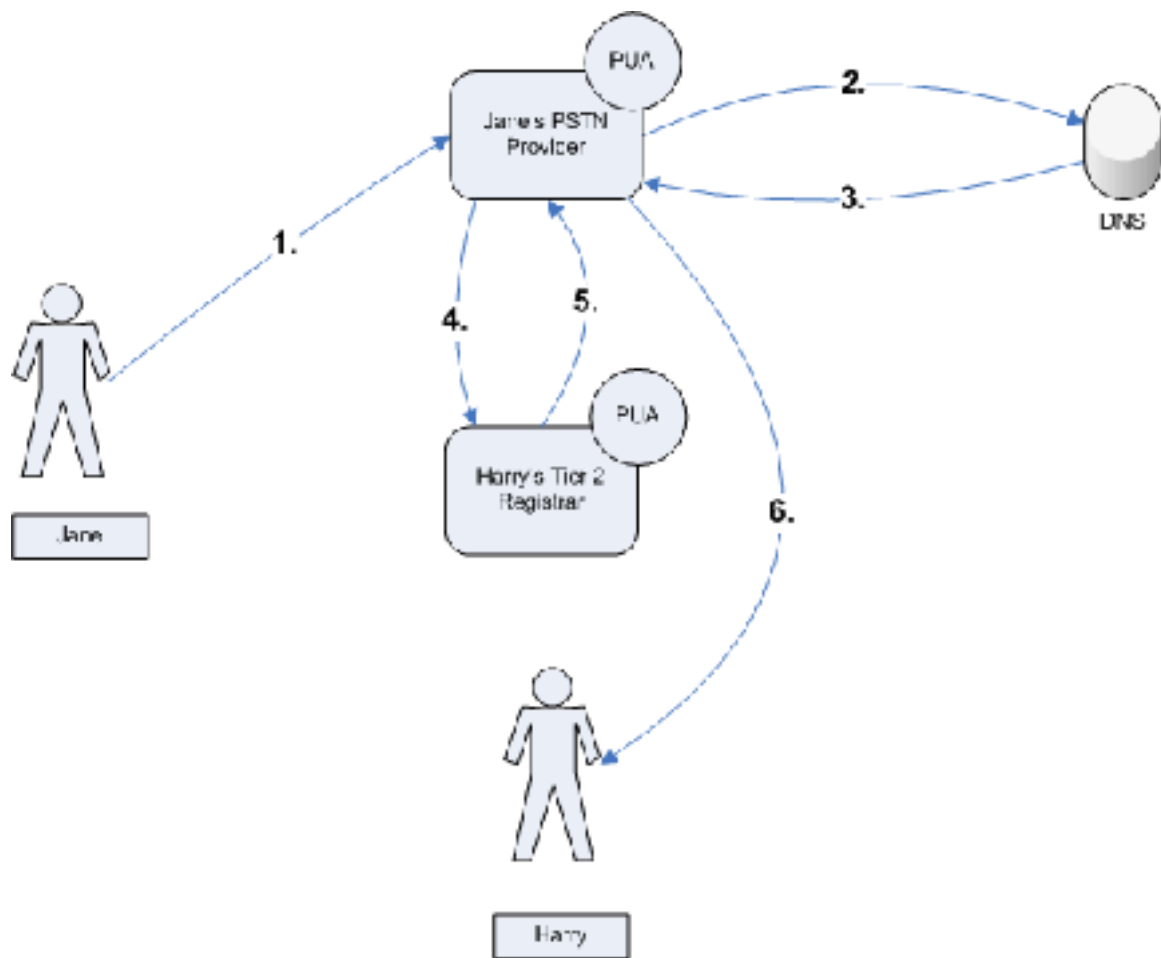
- 5 1. Amanda, the Calling Party, selects Harry's name from her address book and initiates a voice call
2. Amanda's PUA looks up the e164.arpa namespace in the DNS for the ENUM matching Harry's UCI
3. The DNS replies with the URI for Harry's PUA
4. Amanda's PUA requests a voice call from Harry's PUA, supplying Amanda's identity, and indicating that VoIP or traditional telephony is supported
- 10 5. Harry's PUA agrees to initiate an immediate voice call and returns a temporary URI for Harry's VoIP mobile phone
6. Amanda's terminal connects directly to Harry's VOIP mobile phone

8.2.5 Call from a PSTN Provider without an outbound PUA proxy to a UCI



1. Bob, a PSTN customer, dials Harry's number, which is an ENUM
- 5 2. As Bob's PSTN Provider does not have a default PUA that it applies for calls to ENUMs, the call is sent to the Gateway Provider as the PUA of last resort
3. The Gateway Provider's PUA looks up the e164.arpa namespace for the ENUM matching Harry's UCI in the DNS
4. The DNS replies with the URI for Harry's PUA
- 10 5. The Gateway Provider's PUA requests a voice call from Harry's PUA, supplying the CLI information of the original call if available, and indicating that VoIP or traditional telephony is supported
6. Harry's PUA agrees to initiate an immediate voice call, and returns a temporary URI for Harry's VoIP mobile phone
- 15 7. The Gateway Provider connects the call to Harry's VoIP mobile phone, which supports both normal mobile telephony and VoIP

8.2.6 Call from a PSTN Provider with an outbound PUA proxy to a UCI



1. Jane, a PSTN customer, dials Harry's number, which is an ENUM
- 5 2. Jane's PSTN Provider's PUA looks up the e164.arpa namespace for the number in the DNS
3. The DNS replies with the URI for Harry's PUA
4. Jane's PSTN Provider's PUA requests a voice call from Harry's PUA, supplying the CLI information of the original call if available, and indicating that VoIP or traditional telephony is supported
- 10 5. Harry's PUA agrees to initiate an immediate voice call, and returns a temporary URI for Harry's VoIP mobile phone
6. Jane's PSTN provider connects the call to Harry's VoIP mobile phone, using their inhouse PSTN to VoIP gateway

9 Technical system description

9.1 Background – the technical architecture of ENUM

5 ENUM is a service defined by RFC 3761, “[...] by which an E.164 number, as defined in ITU Recommendation E.164, can be expressed as a Fully Qualified Domain Name in a specific Internet Infrastructure domain defined for this purpose (e164.arpa). The result of the ENUM query is a series of DNS NAPTR resource records [RFC2915] which can be used to contact a resource (e.g. URI) associated with that number.”⁷

10 To translate a number to a domain name, for use with the DNS, it must be reversed and a dot placed between each number. For example, the Catalyst IT main number, +64 4 499 2267, would be found in DNS at 7.6.2.2.9.9.4.4.4.6.e164.arpa. Querying this number would return a set of NAPTRs, which can be parsed into URIs for services.⁸

For usage with a PUA and UCI system, each ENUM would return a NAPTR which could be parsed to the URI of a PUA. Multiple NAPTRs may be returned, in which case the first available PUA would be used.

15 9.2 PUA and UCI software architecture

The software architecture described is one based on open standards, and is designed to maximise interoperability between diverse devices.

20 The protocols used will need to be experimented with, and perhaps customised, during the pilot. The intention of the software architecture is to be as open as possible to extension of the core standards, while still maintaining a core set of values that allow even simple devices to participate.

The system consists of:

- Client device, which may provide the human interface for the PUA object
- PUAs, which may provide their own human interface or solely use XML interfaces
- The DNS, which acts as the data store for ENUM
- 25 • A Gateway Provider, to which PSTN calls are routed if the Calling Party does not support VoIP and the Called Party does not support PSTN; or vice versa
- PSTN Providers
- Authentication Authority, which maintains a directory of UCIs

30 PUAs, the DNS, and the Gateway Provider are always network-available. Client devices are not required to be always network-available. The PSTN providers are always reachable using PSTN.

7 <http://www.ietf.org/html.charters/enum-charter.html>

8 RFC 3761: “The output of the last DDDS loop is a Uniform Resource Identifier in its absolute form according to the 'absoluteURI' production in the Collected ABNF found in RFC2396”

9.3 Use of SSL

SSL or TLS will be used to provide privacy and reliability in communications.

- 5 The version of SSL/TLS used will support exchanging digital certificates. These certificates include a distinguishing name, public key, and validity dates. Certificates will be signed by their issuers – for most users, a Tier 2 Registrar. The signer's certificate will also be signed, typically by the Authentication Authority.

The certificate distinguishing name will be in the format:

- E164 format ENUM associated with UCI, followed by a comma,
- the full name of the registrant, followed by a comma,
- 10 • the GMT creation time of the UCI, in YYYY-MM-DD HH24:mm format.

Registrants operating their own PUAs will need to generate their own keys and submit a certificate signing request (CSR) to their Registrar.

Registrars will also generate CSRs for the Authentication Authority, which will be signed as part of the Registrar certification process.

- 15 Each SSL interaction works as:

- The Calling Party provides their SSL certificate
- The Called Party PUA does OCSP queries until they have validated signatures up to a root certificate they trust
- The Called Party PUA provides its SSL certificate
- 20 • The Calling Party PUA does an OCSP queries until they have validated signatures up to a root certificate they trust
- The SSL connection is established

This can be varied so that the calling party does not present a certificate where anonymity is desired.

9.4 System interfaces

- 25 The following internal interfaces exist within the system and are defined below:

- Client device «» PUA
- PUA «» PUA
- PUA «» DNS
- PUA «» Authentication Authority

- 30 The following internal interfaces exist within the system and do not need to be defined:

- Client device «» Client device, which may use any protocol negotiated by their respective PUAs
- Client device «» PSTN Providers, which will use PSTN to communicate
- Client device «» Gateway Provider, which may use any protocol negotiated by their respective PUAs
- 35 • Client device «» DNS, which would use standard DNS if needed
- Gateway «» DNS, which would use standard DNS if needed

- PSTN «» Gateway, which would use standard PSTN
- PSTN «» PSTN, which would use standard PSTN
- Authentication Authority «» DNS, which would use standard DNS if needed

The following internal interfaces do not exist:

- 5 • Client device «» Authentication Authority
- DNS «» DNS, as we treat the DNS as a monolithic entity for this purpose
- Gateway «» PUA, as this would only occur either when the PUA was acting as a Client or the Gateway was represented by a PUA
- Gateway «» Gateway
- 10 • PSTN «» PUA, as a PUA of last resort is provided
- PSTN «» DNS
- Authentication Authority «» Gateway
- Authentication Authority «» PSTN
- Authentication Authority «» Authentication Authority

15 **9.4.1 Client device «» PUA**

Communications between the client device and the PUA could take place using:

- VoIP
- PSTN
- Text message
- 20 • Email
- Picture message (also known as PXT)
- HTML over HTTP
- XML over HTTP

25 Outbound VoIP or PSTN would be used where the client device is “dumb” as far as the PUA is concerned. An example would be a currently deployed analogue cellphone. To reach the PUA, the Calling Party would dial a number, such as “990”. They would then be connected to their PUA, which would use CLI, optionally with PIN, to identify them. In this mode, the PUA would actually have to initiate the communications on their behalf, rather than returning a URI to the calling device.

30 Inbound VoIP or PSTN could be used by the PUA to deliver voice messages, or notify the user of an important event.

Outbound text message could be used for simple interactions with a PUA that required little security, such as querying the current user profile.

35 Incoming text message or picture message could be used to deliver asynchronous communications or notify the user of an event.

Outbound HTML over HTTP would be used when a person is interfacing with a PUA using a web browser. Authentication could be either by shared secret or by client-side SSL certificate. While the Client device to PUA communication would be solely HTTP, communications initiated would use other protocols. It is not anticipated that inbound HTML over HTTP would be used.

XML over HTTP would be used for any non-legacy client. The XML variant to use would be the same as that used for the PUA «» PUA interface below, although different functions would be available. A focus of the XML over HTTP Client device «» PUA interface would be to require little of the client, enabling lightweight technology implementations such as Java Applets. We anticipate it would be technically feasible to implement a client that would operate on some existing cellphones.

9.4.2 PUA «» PUA

PUA to PUA communications will all take place using XML. No specific XML variant is recommended at this point – it is recommended that at the stage of a pilot development, the protocols used by Jabber⁹ be used as a starting point. These protocols support end-to-end signing and object encryption, but will require extensions for PUA requirements.

If the Jabber-based signing and encryption protocols are not used, SSL-based signing and encryption is recommended. An SSL certificate would be generated by the Tier 2 Registrar and would be signed by the Authentication Authority when the UCI is created. This certificate would be used by the PUA object, which would typically be hosted by the Tier 2 Registrar.

It is anticipated that when a contact is added from the UCI Directory their digital certificate is stored by the retrieving PUA.

The process for a PUA to PUA communication, where the destination is specified as a number, would be:

- Calling Party PUA sends a DNS query for the ENUM matching the numeric component of the UCI to their DNS server
- DNS server sends reply to Calling Party PUA
- The Calling Party PUA initiates an SSL connection with the Called Party PUA (see *Use of SSL* above)
- The Calling Party PUA uses the SSL connection to send a request to Called Party PUA for a real-time voice call, sending a prioritised list of supported connection methods, of which lower priority methods will be non-real-time. This connection is retained and used for subsequent PUA-PUA communication.
- Called Party PUA responds to the Calling Party PUA, using the existing connection, to either immediately return a URI or request additional information (e.g. location), and then once a reply is received return a URI
- The Calling Party PUA either returns the URI to the Calling Party PUA Client or initiates the connection itself
- The Calling Party PUA terminates the connection.

9.4.3 PUA «» DNS

PUA to DNS interaction will take place using the ENUM architecture described above. The Calling Party PUA will then contact the Called Party PUA at the URI returned.

⁹ RFCs 3920-3923

9.4.4 PUA «» Authentication Authority

The PUA to Authentication Authority interface would be XML. The XML variant to use would be the same as that used for the PUA «» PUA interface above, although different functions would be available.

5 9.5 Administration processes

9.5.1 Interception, search, and credential recovery

A requirement of the system is that the system operators are able to comply with search warrants or interception orders.

10 To accommodate this, private keys are typically generated by each Tier 2 Registrar, signed by them, and their key signed by the Authentication Authority. This would allow the Tier 2 Registrar to comply with requests to capture and provide in plain text any traffic to or from a PUA.

15 As the keys are not used by client devices, this will not facilitate interception of client to client communications, which may be encrypted using another set of keys. As those services are not provided by the PUA and UCI system, facilitating interception of these communications is not a design requirement.

As the private key is not used on a client device, users should not lose access to their private keys unless through Registrar failure. The Authentication Authority can remedy Registrar failure by revoking their signature upon the Registrar's key, and signing a new key generated by the Registrar.

20 A small number of people will wish to operate their own PUAs, and they will generate their own keys. Interception of their PUA traffic would require compromise of their system, or monitoring from the other end of communications they initiate. These users would generate certificate signing requests so their Registrar could sign their keys.

25 In the case of the Authentication Authority being compromised, the root key on all client devices will need to be updated. While this would be cumbersome, it should be achievable if designed into client devices. A new Authentication Authority key would need to be generated and would then re-sign all the Tier 2 Registrar keys.

9.6 Operating a PUA server

30 Operating a PUA large-scale server would provide challenges, due to the potentially large client base. A reasonable medium-term scenario would be for one company to gain 80% of a four million person market.

PUA software will have a higher rate of change than mail server software, and connections to clients will be persistent. A large scale implementation will therefore need substantial load balancing.

The load balancing architecture proposed would be:

35 1. Client connects to URI which may be round-robin to any of n servers, without session-aware load balancing

2. Server returns URI of specific machine or cluster: load balancing from this point must be session-aware
3. Client initiates persistent XML connection

This architecture would support millions of connections on generic i386-based hardware.

10 Glossary

CLI	Caller Line Identity: a system that provides the telephone number of the Calling Party to the Called Party in traditional telephony. CLI is commonplace in digital mobile telephony.
NAPTR	A type of DNS record that can be processed to provide a URI.
OCSP	Online Certificate Status Protocol, defined by RFC 2560.
PSTN	Public Switched Telephone Network: the world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. Also called POTS. ¹⁰
spam	Unsolicited communications.
SSL	Secure Socket Layer: an open protocol used to implement public key cryptography, providing privacy and sender verification. We include TLS (the Transport Layer Security protocol) when we refer to SSL, as this is the name that new versions of SSL will be known as.
URI	Uniform Resource Identifier: the address of a resource, typically on the Internet, together with a code for the protocol to use to access it.
URL	Uniform Resource Locator: a form of URI used for the HTTP protocol.
VoIP	Voice over Internet Protocol.

11 Document status and version history

- 5 This document has been produced in response to the InternetNZ document “Terms of Reference for Feasibility Study” version 1.1 (ToR). The ToR document lists a number of assumptions, such as the use of DNSsec, which affect feasibility.

The time allocated to the feasibility study is two to four person weeks.

Within these constraints, this document represents the professional opinion of Catalyst IT as to the feasibility of the Personal User Agent and Universal Communications Identifier technologies.

- 10 This document has been researched and written by Peter C. Kelly.

Document version history:

<i>Version</i>	<i>Date</i>	<i>Description</i>
0.1	9 Jan 2005	Early work in progress version released for internal progress update.
0.2	11 Jan 2005	Trivial changes from 0.1, presented to client to stimulate discussion
0.3	18 Jan 2005	Further development throughout paper. Incorporates client feedback on version 0.2
0.4	21 Jan 2005	Draft presented to client for in-progress review.
0.8	2 Feb 2005	Draft presented to client for ToR checkoff
0.9	3 Feb 2005	Draft for formal client review
1.0	10 Feb 2005	Document completion
1.1	5 Apr 2005	Minor grammatical and typographical amendments.

¹⁰ <http://www.cit.nih.gov/dnst/handbook/Main/glossary>

12 Bibliography

- M. Sutton, ToR for Feasibility Study, ENUM Steering Group, 24/12/04
- ICANN Public Forum Transcript Morning 25 March 2003, ICANN, 25/3/2003
- ETSI EG 202 067 UCI System Framework v 1.1.1, ETSI, 9/2002
- 5 ETSI EG 203 072 UCI study for NGN v. 1.1.1, ETSI, 11/2003
- ETSI TR 103 077 Universal Communications Identifier (UCI); Maximizing the usability of UCI based systems v 1.1.1, ETSI, 1/11/2002
- Enum Forum Working Document #6000_1_0, ENUM Forum, 14/3/2003
- 10 Draft determination on the multi-party application for determination of local telephone number portability service and cellular telephone number portability service designated multinet network services, Commerce Commission, 6/12/2004
- Introduction of ENUM in Australia, Australian Communications Authority, 9/2002
- M. Pluke, Universal Communications Identifier (UCI), ETSI, 5/2002
- A Newton, An ENUM Registry Type for the Internet Registry Information Service, IETF, 1/2005

13 Appendix: Terms of Reference

Introduction:

5 International Enum Forums and organizations have identified security and privacy as critical to the integrity of the Enum Tier 1 and Tier 2 systems. Substantive recommendations are available for the Steering Group to use as a basis for implementing core Enum Tier 1 and Tier 2 systems.

10 These international studies were not tasked with addressing the operational privacy and security of clients. It was reported that controlling client Calling and Called Party permissions and access would be critical to the public and corporate adoption of Enum as meaningful services. Participants have suggested that solutions could be found through several methods best defined as **Personal User Agents (PUA)** and **Universal Communications Identifiers (UCI)**. These dynamically control access to the discrete information contained within Enum records, depending on the Calling Party identity and permissions set by the Called Party.

15 UCI offers Enum clients a long-term individual identity. UCI might be used with SSL certificates to control PUA, aggregate international Enum(s) and provide, as a Calling Party, an SSL signature as a personal identifier that can be used to determine which Enum profile will be presented by the Called Parties PUA.

Objectives:

20 This Feasibility Study is to make specific and constructive recommendations:

Objective 1:

- Define how (generally) to implement and operate **Personal Users Agents (PUA)** software within an operational Enum system. Identify software that may fulfil the functional capability and suggest any which might be modified to support Enum trials.

25 **Objective 2:**

- Define how to implement and operate **Universal Communications Identifiers (UCI)** in conjunction with PUA and the core Enum Registry system to support each individuals long-term personal identity on which they can associate Enum identities with and have ownership rights over.

30 **Objective 3:**

- Describe how end users could remotely modify their PUA profile on demand using their UCI identity and SSL certificates to provide operational flexibility and confidence that their profile is secure from unauthorized modification. Describe how an UCI SSL certificate could be used to confirm a Calling Party's identity to validate an Enum request to a PUA.

35 **TASKS: Feasibility Study is required to address :**

1. Make specific and constructive recommendations in respect of Objectives 1-3.

Ensure that the following are explicitly addressed: (see addendum)

2. Are PUA viable? – why, and how to enable
3. Will PUA aid end user security? – why and how
- 40 4. What are the security implications for not implementing a PUA system? - detail
5. Can PUA respond to Enum requests not represented by a PUA? - describe

6. Describe PUA software architecture? - detail
7. Name existing PUA software? (proprietary and Open Source) - specify
8. Is it possible to build PUA's on to existing DNS server software? - describe
- 5 9. Is it possible for lite-versions of PUA to be built, such as Java applets for handsets? - describe
10. How might SSL certificates be used to sign requests for PUA services Calling and Called Party? - describe
11. How might a large scale PUA be built. Do they offer the hosts commercial opportunities? – describe
- 10 12. Are UCI records viable for use with PUA? – how and why
13. Are UCI records easy to construct? – how and why
14. How might UCI records be generated by AA and exchanged to Registrants and Registrars? – describe
- 15 15. How can SSL certificates and other identity methodologies be used in real-time to validate the Calling Party? - describe
16. Is it possible for client HTML type directory inquiries to use SSL or other tags to communicate with the PUA Servers to establish identities? - describe
- 20 17. What are the benefits and requirements for hosting an On-Line Certificate Status Protocol (OSCP) database to provide Certification Revocation List disclosure with pre-produced signed responses enabled? – describe
18. What are the best practices other Industry groups may utilize to establish a similar service? – comment

Assumptions:

- 25 For the purpose of developing this Report: It is to be assumed that the New Zealand Enum Steering Group, with agreement from the NAD and Government, has decided to implement an Enum Registry Tier One and Tier Two system, comprising:
 - A **single Tier 1** Registry operated by InternetNZ.
 - A **single** Enum establishment **Authentication Authority (AA)** operated by InternetNZ.
 - 30 • An Enum establishment **Appeal Process** would be provided. (address applications rejected by the AA)
 - A **competitive** SRS based **Tier 2** Registrar system with **multiple Registrars**.
 - Telecommunication companies would chose to **opt-in** to the Enum authentication and establishment process.
 - 35 • Any telephone user will be able to apply to establish Enum identity. Clients of non-participating companies will be permitted to provide sufficient identification to the AA to enable Enum approval.
 - **UCI** is a proposal by ETSI that defines itself as a future standalone service which Enum could today benefit from by using parts of the features proposed within UCI.
 - 40 • When a request for an Enum is accepted for registration by a “first time” registrant a UCI with a unique SSL key would be created by the AA. The UCI and Public Key will be passed

to the Tier 1 Registry Tier 2 Registrars with the Enum as a signed Electronic Transaction by the AA. The AA would also pass to the registrant the UCI, Enum, Private and Public SSL client-key for the UCI. The key components might be downloaded from a secure web site and other systems. The UCI Private Key might then be used to transparently and dynamically authenticate / change the PUA settings as well as sign their own Calling Party requests to another PUA they had previously established access permissions with.

- Enum records will be approved for **non-telephone services**.
- The Registry, Authentication center and Registrars would use **DNSsec** (Production mode).
- DNSsec may not be supported contiguously to all parts of the network.
- **IPv6** will be supported ASAP (eg mobile Ipv6).
- UCI Client **SSL Certificates** would be issued by the Authentication Authority as a Certificate Authority.
- Enum will be an **Opt-in** service. User details will only be entered when a user contracts for Enum services.

If a PUA service is deemed viable:

- The **default** configuration will be that each Enum registration will be loaded into the Tier 2 Registrars PUA management system.
 - Registrants may then **transfer** their Enum PUA Management to another service provider or an internal corporate PUA or a private PUA. Or;
 - Registrants must **Opt-out** of the PUA management system in order to utilize the raw Enum DNS system. Registrants may do this for technical and operational reasons where the Enum is a commercial marketing number that requires maximum visibility, nationally and internationally.
- A UCI record is defined as being a concatenation of (may be modified):
 - A numeric e164 number (The first Enum applied for) 644759235; plus
 - The Registrants Name (MichaelSewardSutton); plus
 - A (hidden) hash field unique value such as the time the record was created or an MD5 of the above

30 Security assumptions and caveats

- Enum Tier 1, Tier 2, the Authentication, Appeal system, UCI Database, Certificate Authority and Certificate Revocation database would be commercially secure systems, matching or exceeding the SRS DNS system
- Zone information will be protected from opportunistic and unauthorized access.
- The operational Agreement signed by Tier 2 Registrars will require the use of DNSsec and facilities such as PUA and UCI with OPT-in and OPT-out requirements. It is assumed that breaches of the signed operational Agreement will result in sanctions such as suspension of Registrar rights.
- Individual customer Enum services will not be certified as secure. While DNSsec, SSL and other facilities will support secure operation, it is beyond the scope of this proposal to implement an absolute secure client network facility.

- Without PUA all Enum data stored would be returned to any Calling Party request.
 - PUAs will enable information requests to be filtered providing a dynamic white list facility.
 - The sophistication of the PUA will control how the Calling party is able to identify itself by different mechanisms such as Logon account rights, CallerID SSL etc.
- 5
- SSL certificates could be used and in the New Zealand context. Those who have Enum records would have an SSL certificate issued by the AA (public and private) which can then be used for validation in a PUA session. Called Parties would then be able to choose to “trust” a Calling Parties signed request provided and decide whether to enable that person to be able to receive full or part access to their Enum records. (International SSL public certificates could also be used)
- 10
- The Calling Party may be identified by different mechanisms such as Logon account rights, CallerID.

Terms

Catalyst will assign the following individuals:

- 15
- Dean Barnett – Project Manager
 - David Zanetti – Systems Administrator, Team Leader
 - Andrew Ruthven – Senior Developer
 - Peter Kelly – Researcher

InternetNZ Project Manager and Sponsor is Michael Sutton.

20 The Feasibility Study is to be completed for the fixed price specified in Point 5 of the Application for Funding by CatalystIT.

Unless otherwise agreed, a draft Report will be available on Monday 14th February 2005, with the Final Report available on Friday 18th February 2005.

25 Where it is found that a Task Point is beyond the capability of CatalystIT to address with the agreement of InternetNZ it is to be held-over to ensure that all other Task Points and Objectives are addressed within the allocated time and budget.

The InternetNZ Council has approved funding on the 18th of December 2004.

InternetNZ may release this Report, in part or whole, into the Public Domain.

Signed

30 **CatalystIT** []

Signed

InternetNZ []

Project Sponsor: Michael Sutton (Councillor - Chairman Enum Steering Group)

Date: []

35 References:

A collection of Enum documents downloaded from various sources is available at:

For Enum

<http://www.ietf.org/html.charters/enum-charter.html>

<http://pda.etsi.org/pda> Search for UCI

also for a wide set of Enum references

<http://www.awacs.co.nz/internetnz/Enum/>

Please review documents in <http://www.awacs.co.nz/internetnz/Enum/UCI/>

- 5 An example of a Shared Registry Service system framework as proposed for the United States is available at:

http://www.awacs.co.nz/internetnz/Enum/UCI/etsi_UCI_sys_framework_eg_202067v010101p.pdf

Also: The transcript of presenters at the ICANN meeting on Enum.

- 10 <http://www.icann.org/riodejaneiro/captioning-public-forum-25mar03.htm> transcript

Powerpoints <http://www.icann.org/riodejaneiro/index.html> see agenda links

Addendum:

- 15 At a meeting with Dean Barnett, David Zannetti, Andrew Ruthven of CatalystIT and Michael Sutton on the 7th of January 2005 it was agreed that the boundaries of specific Task objective and assumptions can be broadened to assist ensure recommendations best meet the objectives of this Feasibility Study.

Issues that this applied to related to:

Task 16: HTML Browser enquiries.

- 20 Private Key storage (escrow) by the Authentication Authority and how to best support end users reconstruct their Private Key identity following the loss, damage or theft of an Enum enabled device where the user has not privately backed up their Private key.

Implications for government agency access to information stored within the PUA and UCI

Address application of UCI and PUA to support prepaid mobile cell-phone users.