Telecommunications Carriers' Forum Incorporated

Report for ENUM in New Zealand

Table of Contents

1. EXECUTIVE SUMMARY 4
2. GLOSSARY OF TERMS 6
3. INTRODUCTION 9
4. ENUM EXPLAINED 10
5. TYPES OF ENUM 12
5.1 User ENUM 12
5.2 Infrastructure/Carrier ENUM 12
5.3 Public & Private Infrastructure ENUM 13
5.4 Domain choice for Infrastructure ENUM 13
5.5 Functional Model 13
5.6 Tier 0 14
5.7 Tier 1 Registry 14
5.8 Tier 2 Nameserver Provider & Registrar 14
5.9 Types of Infrastructure ENUM 15
5.9.1 CSP–internal Infrastructure ENUM 15
5.9.2 CSP–shared Infrastructure ENUM 15
5.9.3 Global (or Common) Infrastructure ENUM 16
5.10 Architectural Options 16
6. SUMMARY OF EXISTING ENUM TRIALS 17
7. STANDARDS BODIES UPDATE 20
7.1 ENUM WG (Overview of IETF & ETSI) 20
7.2 Infrastructure ENUM Standards Activities (GSM) 21
7.3 Infrastructure ENUM Standards Activities (ETSI) 22
7.4 UK ETG (ENUM Trial Group) 23
7.4.1 CRUE 23
8. REGULATORY IMPACT 25
8.1 LMNP Codes & Anti-Spam Code 25
9. MAJOR ISSUES 26
9.1 Wider Political Considerations 26
9.2 Known Subscriber Issues 26
10. MAJOR RISKS 28
10.1 Service Integrity 28
10.2 Example Violations of Service Integrity 28
10.2.1 Toll-Free number points to a tel URI associated with a call resulting in toll charges. 28
10.2.2 Geographic number local to the caller location points to a tel URI associated with an international call 29
10.2.3 Maintaining Service Integrity 29
10.3 Validation 29
10.4 Removal of E.164 Numbers 32
10.5 Authentication 32
10.6 Accreditation 33
11. ENUM INTEROPERABILITY 35
11.1 One to One Services 36
11.2 Traditional Basic Calls including SIP Based Services 36
11.3 Converted Application Services 37
11.4 Extended One-to-One Services 38
11.5 Advanced Services 38
11.6 Maintenance services 39
11.7 Services – a general model 39
11.8 Remuneration 39

11.9 Potential list of Originators and Terminators 39
12. ENUM TRIAL PLANNING 41
12.1 Stage 1 Objectives Prior to a Trial 41
12.2 Stage 2 Objectives of an ENUM Trial 41
12.3 Responsibilities of Parties 42
12.4 Scenarios for a New Zealand Trial 44
12.5 High Level Work Plan 45
12.6 INF_ENUM – Infrastructure and ITU delegation. 45
12.7 DOM_ENUM – ENUM domain names and customer process. 46
12.8 APP_ENUM – Applications 46
13. NEXT STEPS 47
13.1 Current (Traditional) Situation on the PSTN 47
13.2 Step 1: CSP Islands connected via PSTN 47
13.3 Step 2: Private Infrastructure ENUM only 47
13.4 Step 3: Private Infrastructure with IP based Interconnect 47
13.5 Step 4: CSP-shared Infrastructure ENUM with Extranet between a Group of Service Providers 48
13.6 Step 5a: Common Infrastructure ENUM within a Global Shared Extranet 48
13.7 Step 5b: Public Infrastructure ENUM on the Internet. 49
14. CONCLUSIONS 50
14.1 Summary of Trials: 50
14.2 Potential Effects of ENUM on Current and Draft Codes 51
14.3 Transition and Interoperability Issues 51
14.4 Numbering 51
14.5 Assignment of the New Zealand ENUM Delegation (.4.6.e164.arpa) 52
14.6 ENUM Registry Structure and Policy Framework 52
15. REFERENCES 53
APPENDICES: 56
APPENDIX A: Draft ETSI TR 102 055 (2005-01) - Infrastructure ENUM 56
APPENDIX B: AUSTRALIA 66
APPENDIX C: UNITED STATES 69
APPENDIX D: UNITED KINGDOM 73
APPENDIX E: NETHERLANDS 77
APPENDIX F: FRANCE 78
APPENDIX G: SWEDEN 80
APPENDIX H: AUSTRIA 81
APPENDIX I: CANADA 84
APPENDIX J: UK ENUM Trial Group (UKETG) Report May 2004 86
APPENDIX K: TCF ENUM Working Party Project Scope 93

1. EXECUTIVE SUMMARY

Internationally ENUM has evolved rapidly in both the standards arena and in its industry forms in the 12 months since Internet New Zealand's report first mooted a New Zealand User ENUM trial. Standards first ratified two years ago have been edited and updated, and are about to be ratified. Industry forms have morphed through experience gained in overseas trials and in recognition that ENUM's various flavours need to coexist, and may need to cooperate in some way. Additional topics such as VoIP peering have emerged that may alter the ENUM landscape. And, as yet there is no unified approach on or understanding of ENUM between the internet IETF and ITU / telecommunications communities.

Overseas, some findings from trials are that no known business case exists for ENUM and that privacy concerns have restricted many trials to VoIP only i.e. no PSTN. In Austria, one of the 3 countries that are commercially using ENUM, the basic lesson is "you cannot sell ENUM". Common privacy concerns include identity theft and spam and there are issues with the "opt-in" model required with User ENUM. In the United Kingdom, perhaps one of the most advanced examples of ENUM trials and experience globally, four major issues after 4 years of trial are:

- authentication i.e. identification and validation of identity to meet user privacy;
- policy formation e.g. who develops policy, can it be enforced and by whom;
- tier 1 (registry) selection e.g. who pays, who takes responsibility, what commercial model will be used; and
- separate number range e.g. issues with geographic and non-geographic numbers.

These are fundamental issues which are either as yet unaddressed or unsolved in the UK and other trials.

From an offshore regulatory standpoint, no regulation is in place or planned for ENUM in any of its forms. However, many overseas regulators are interested in, and in some countries actively involved in, ENUM.

The Internet New Zealand report dated April 2005 proposed a User ENUM trial of the type already performed in multiple countries. The ENUM Working Party's (Working Party) conclusion is that, in its current form, this trial will not add anything to that which has not already been proven overseas. Nor will it address key concerns such as those found overseas and echoed by this Working Party. Any trial in New Zealand should encompass both User and Infrastructure (Carrier) ENUM, include both the Internet and telecommunications communities where appropriate and determine policy, principles, governance, codes of practice, legal requirements including enforcement, customer requirements including privacy and an appropriate model including architecture, registry / registrar interactions and domain trees prior to the trial commencing.

The Working Party considers that New Zealand should capitalize on the lessons learned overseas through active participation in the standards bodies ENUM working parties for both ETSI and IETF as well as those for VoIP peering and in country specific Infrastructure ENUM initiatives such as CRUE (UK). This alone will take significant resource but will prevent New Zealand repeating the mistakes and limited outcomes of overseas trials and may speed up the eventual implementation and use of ENUM in New Zealand.

Some overseas experience links ENUM and future number portability. The Working

Party recommends that any ENUM trial commence after implementation of number portability in New Zealand. While some synergies may exist, the increased risks and unknowns inherent in the currently evolving ENUM landscape would significantly delay the implementation of number portability. Overseas experience has also shown that a working number portability database of the type in development in New Zealand aids the implementation of ENUM.

The Working Party considers that, to progress ENUM, significant resource needs to be committed in three stages. Stage 1, before April 2007, should include active participation in international standards bodies and working parties relevant to ENUM and development of high level policy, principles, codes of practice, legal requirements including enforcement and customer requirements including privacy and define, if possible, a business case for ENUM.

Stage 2 should, building on stage 1, determine the objectives, requirements and responsibilities for a trial and define architecture, registry / registrar models and other design requirements including interoperability and interconnection. This would aim to build on overseas experience. Refer to Section 12.5 for an example ENUM work plan to encompass stage 1-2.s

Stage 3 would be the actual trial at a yet to be determined date.

Finally, on the request for delegation of the 4.6.e164.arpa delegation, the Working Party recommends that this delegation continue to be held by the Ministry of Economic Development (MED) until a trial, as outlined in this report, begins or unless Internet New Zealand and the TCF Board jointly agree differently.

2. GLOSSARY OF TERMS

Below are definitions and descriptions of some of the central terms and concepts.

Term	Definition
ACA	Australian Communications Authority.
ACIF	Australian Communications Industry Forum.
AoR	Address of Record
APF	Anti-Privatisation Form
ASP	Application Service Provider.
Basic Call	Loosely; to perform a telephony (voice) conversation between two parties including the signalling necessary to setup the call and terminate it.
CDMA	A technology for digital transmission of radio signals between, for example, a mobile telephone and a radio base station. In CDMA, a frequency is divided into a number of codes.
CDR	Call Detail Record
CRUE	Carrier Registration in User ENUM
CSP	Communications Service Provider.
DNS	Internet service that translates domain names into IP addresses.
E.164 numbers	E.164 is an international numbering plan (originally developed by the ITU) for public telephone systems in which each assigned number contains a country code (CC), a national destination code (NDC), and a subscriber number (SN). The administration of the national numbering plan below the Country Code level is a matter for each country holding the E.164 delegation. This is typically carried out in accordance with ITU Recommendation E.129 – Presentation of national numbering plans.
EFA	Electronic Frontiers Australia
ENUM	A procedure that processes an E.164 telephone number to map it to a ENUM domain name and subsequently extracts record from that domain returning a list of other E.164 related identities to the calling procedure containing for example telephone numbers (tel-URL), e-mail addresses, web addresses and other URLs.
ETSI	European Telecommunications Standards Institute.
GPRS	General Packet Radio Service, a GSM data transmission technique that does not set up a continuous channel from a portable terminal for the transmission and reception of data, but transmits and receives data in packets.
FCC	Federal Communications Commission (United States Regulatory body).
GRX	Global Roaming Exchange.
GSM	Global System for Mobile Communication, a widely used digital mobile phone standard.
GSMA	GSM Association.
IAB	The Internet Architecture Board is a committee of the Internet Engineering Task Force (IETF).
IMS	Instant Messaging Services for fixed line and mobile devices.
IMSI	International Mobile Subscriber Identity.
IP	The protocol by which data is sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. IP is a connectionless

	protocol, which means that there is no established connection between the end points that are communicating.
IPX	Enhanced GRX.
IREG	International Roaming Expert Group under the GSMA auspices.
ITEF	Internet Engineering Task Force.
ISDN	Integrated Services Digital Network, an international standard for end-to-end digital transmission of voice, data, and signaling.
ITU	The International Telecommunication Union: http://www.itu.int/aboutitu/index.html.
LDAP	LDAP is a software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the Internet or intranet.
LMNP	Local and Mobile Number Portability as defined under the LMNP and Network Terms. Launches April 1st 2007 as determined by the New Zealand Commerce Commission.
MED	Ministry of Economic Development (New Zealand Government Department).
MMS	Multimedia Message Service, a method of transmitting graphics, video clips, sound files, text messages over wireless networks using the WAP protocol.
MNO (s)	Mobile Network Operator (s).
MOLI	Mobile Origin Location Indication.
MoU	Memorandum of Understanding. A statement specifying agreement relative to responsibilities and authorities on matters on common interest.
NAD	Number Administration Deed.
NAPTR	Naming Authority Pointer and is a newer type of DNS record that supports regular expression based rewriting.
NAT	Network Address Translation is typically used between RFC1918 private addressing and real world Internet address space. But can encompass the translation mechanism IPv4 and IPv6.
NCC	Network Control Center, a central location on a network where remote diagnostics and network management are controlled.
NMT	Nordic Mobile Telephone. An analogue (1G) cellular system that used either the 450 MHz or 900 MHz bands. It was developed for deployment in Scandinavia, but its use spread to many other countries. It was the first cellular system to be used commercially.
NGN	Next Generation Network (typically refers to a high bandwidth or Ipv6 network).
NNPA	National Number Plan Administrator.
NPA	Numbering Plan Area — another term for an area code.
PABX	A small switching system installed on a business customer's premises which provides internal telephone switching, as well as outside connections. The system can be either mechanically or electronically controlled.
PLMN	Public land mobile network is a network that is established and operated by an administration or by a recognized operating agency (ROA) for the specific purpose of providing land mobile telecommunications services to the public.
PoI	Point of Interconnect. The point in a carrier's network at which signaling and voice/data traffic is passed to other networks, where commercial arrangements are in place.
PSTN	Public Switched Telephone Network.

PUA	Personal User Agent.
P2T	Push to Talk. A feature that is available on certain more recent mobile phone models. It allows the mobile phone, when in a special mode, to function as a digital two-way radio in push-to-talk operation.
RIPE	A collaboration between European networks which use the TCP/IP protocol suite.
RFC	The name of the result and the process for creating a standard on the Internet. New standards are proposed and published on the Internet, as a Request For Comments.
SIP	The Session Initiation Protocol (IETF standard RFC 3261), is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, chat, interactive games, and virtual reality. SIP was developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, with work proceeding since September 1999 in the IETF SIP working group. See i e http://www.cs.columbia.edu/sip/ and http://www.ietf.org/html.charters/sip-charter.html.
SMS	Short Message Service - Short text messages that can be sent to a mobile phone.
SPEER	SIP peering and VoIP peering working groups amalgamated into the SPEER working group, under the IETF framework.
SPEERMINT	Session Peering for Multimedia Interconnect (IETF working group formed in March 2006).
TCF	The Telecommunications Carriers' Forum.
TCP	Transmission Control Protocol, is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
TDM	Time Division Multiplexing is a scheme in which numerous signals are combined for transmission on a single communications line or channel. Each signal is broken up into many segments, each having very short duration.
TLD	Top Level Domain. The first level of an Internet site address.
ccTLD	In the case of ENUM or wider Internet – Country Code Top Level Domain such as .co.nz or .com.au.
TSP	Telephone service provider.
UKETG	UK ENUM Trial Group.
UMTS	Universal Mobile Telecommunications System. A globally standardised system for mobile telephony and data communication.
UPT	Universal Personal Telecommunications Service.
URI	The Uniform Resource Identifier, which is a generic term for all kinds of object-identifiers used on the Internet, including web page addresses (URLs) and email addresses.
VoIP	Voice over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

3. INTRODUCTION

In September 2005, the Telecommunication Carrier Forum Incorporated (TCF) established the Working Party to investigate how the implementation of ENUM within New Zealand would affect the Telecommunications industry and its customers. During our information gathering exercise for this report, the Independent Chair of the TCF tabled the Minister of Communications to request deferment of the E.164.ENUM delegation authority for New Zealand, by the Ministry of Economic Development (MED), until the TCF ENUM findings are concluded. This was acknowledged formally by the Minister in a letter dated 5 January 2006.

The evolution of telecommunications today includes the traditional fixed line telephony services, the Internet, mobile networks, and what are known as converged services that include a mixture of each network The global evolution of ENUM is adding to this within the PSTN, broadband, and mobile environments but on a compressed timescale due to the rapid uptake of VoIP technology. Essentially, ENUM carries the promise of enabling new features which overlay these traditional networks. However, because ENUM is an IETF standard based on IP technology, and the PSTN and mobile networks are based on telecommunication standards using sets of protocols other than IP, the standards are in many ways contradictory and can impose significant challenges during a trial or eventual live deployment. Over the past 5 years, this has certainly been the case worldwide.

At first glance ENUM may seem a simple protocol, but its arrival and use raises a number of issues for the New Zealand telecommunications and Internet communities that need to be addressed before any real deployment can take place.

Those overseas ENUM trials which have so far occurred have all been completed with limited outcomes in terms of tangible results that can be used within a live / commercial deployment scenario. A common outcome from these usually User ENUM trials was an acknowledgement that associated codes of practice, regulatory and governance, technical and commercial standards need to emerge prior to a successful infrastructure ENUM trial occurring.

This report has been written to encompass the lessons learned from overseas trials, interpret these in the New Zealand context and recommend how ENUM should proceed from a TCF perspective.

In the future, and subject to agreement by the TCF Board, the Working Party is committed to ensuring that the necessary policy and governance is implemented prior to undertaking a successful trial of Infrastructure ENUM in New Zealand, and has actively probed members to participate in the ENUM education process during the report preparation phase. The Working Party has very real concerns about the security of any User ENUM trial, in view of the later arrival (post number portability) of Operator/Infrastructure ENUM in New Zealand.

This report begins with an outline headed “what is ENUM”, contains a summary of findings, experiences and outcomes as well as progress of overseas ENUM trials, discusses the rapid evolution of ENUM from both standards and industry viewpoints, raises key issues and risks with ENUM, and provides an example of requirements for a trial and gives a number of conclusions and recommendations for board consideration and action.

4. ENUM EXPLAINED

The original ENUM specification is contained within the IETF Request For Comment (RFC) document, RFC 2916 (IETF 2000). Note: RFC 2916 is now obsolete and is superseded by RFC 3761 (April 2004).

In RFC 2916, ENUM is described as *"the use of the Domain Name System (DNS) for storage of E.164 numbers"*. ITU-T Recommendation E.164 is the International Telecommunication Union (ITU) standard that defines the format for telephone numbers. ITU-T Recommendation E.164 enables telephone numbers to be assigned to devices in countries throughout the world, so as to achieve uniqueness, and enable reliable selection of a desired device to connect to by means of the Public Switched Telephone Network (PSTN).

ENUM is intended to establish a mechanism whereby E.164 numbers can be mapped to the IP-address of a device located on an IP network (e.g., public Internet, or private Intranet). Specifically, ENUM, as per RFC3761 clause 1.2 involves mapping E.164 numbers to the e164.arpa domain. For example, the telephone number +64-4-4720030 would translate to the domain 0.3.0.0.2.7.4.4.4.6.e164.arpa.

ENUM is not an application in itself, but rather an underlying enabler for applications. The primary use of ENUM to date has been for voice, because Voice over IP (VoIP) usage is rapidly expanding. However, should the development community get behind the global ENUM initiative, it could eventually be used as part of Instant Messaging, Universal Follow Me, or Location Based Services scenario.

ENUM also enables telephone numbers to be used as service identifiers, defined as Uniform Resource Identifiers (URIs), on the Internet. URIs are identifiers of IP end-points (e.g., end-clients, servers, applications) connected to an IP network (e.g., the Internet) and can take a range of formats (e.g., web-address, email addresses).

The scope is actually much broader than simplified descriptions like the one above outline. More fully, "ENUM enables the use of phone numbers as identifiers of services defined as URIs on the Internet as well as facilitating the interconnection of systems that rely on telephone numbers with those that use URIs to route transactions". URI is a generic term for all kinds of object-identifiers used on the Internet, including web-page addresses (correctly called URLs) and email-addresses.

As generic as this above service description is, the proposed ENUM technical descriptions as expressed in RFCs 2915 and 2916 were fairly vague, and essentially defined data structures but did not populate them with real life scenarios. This vagueness with the earlier ENUM RFCs (prior to User and Infrastructure ENUM drafts expiring in April 2006) explains a lot when illustrating some of the early trials undertaken in both the USA and Europe. Each of the early trials struggled due to a lack of policy, governance, regulatory planning, and a concerted subscriber and developer education program during the trial period. Some industry strategists suggest it is simply a by-product of applying the design technique sometimes referred to as 'top-down with step-wise refinement', leaving many details for subsequent articulation in the field.

Anyone can use or implement ENUM today and some service providers are using it internally, without exposing their data to the outside world. That this occurs illustrates the vagueness inherent in the ENUM descriptions.

As it stands today, considerable activity is being undertaken by industry associations and standards bodies to seriously evolve ENUM so as to harmonize national number plans within each country, with validated ENUM endpoints, to remove the vagueness that characterized its initial description and to endeavour to standardize the use of and various flavours of ENUM actually in use. Many of the current ENUM technical proposals in the public domain, both within ETSI, the ITU, the IETF, and the wider Internet community, have been fraught with technical problems relating to authentication, validation and subscriber privacy. With increased IP mobility and peer-2-peer styled VoIP services being undertaken globally, the challenges outlined within this report have attracted a great deal of previous international criticism on those grounds alone. Our conclusions and recommendations will be in direct reference to the public interest aspects of a future ENUM initiative; particularly its privacy implications; but also the potential industry and customer impact should the telecommunications operators not implement a suitable ENUM structure to cope with varying levels of industry and consumer demand, whilst still maintaining the integrity of New Zealand's national number plan.

5. TYPES OF ENUM

There are a number of types of ENUM and confusingly, a number of different terms optionally used to describe those types. This often makes it difficult to determine what ENUM is being described in published documents and obviates understanding. Some of the terms used to describe ENUM are – User, Infrastructure, Carrier, Operator, Enterprise, Corporate, Federated, Public, Private.

We have restricted the terms we use to:

- User ENUM, which by definition can only be Public; and
- Infrastructure/Carrier (aka Operator) which can be either Private or Public.

5.1 User ENUM

User ENUM (also called Public ENUM) allows end users to link their existing E.164 numbers to applications on the internet, reachable via URIs.

In User ENUM, it is the choice of the end user or ENUM subscriber to enter information (resource records or NAPTRs) into their assigned ENUM domain. This is more commonly known as the "opt-in" principle.

User ENUM typically exists on the public Internet, and uses public DNS. Therefore all information in User ENUM is publicly accessible. This introduces privacy concerns which are discussed later in this report.

5.2 Infrastructure/Carrier ENUM

Infrastructure ENUM, also called Carrier ENUM, is essentially about publishing which E.164 numbers a Communications Service Provider (CSP) is hosting to either a group of selected peers or to all other CSPs.

It is used to facilitate the routing between CSPs to border elements of other networks (e.g. a switch, an egress gateway, a point of interconnect to another network, etc).

Comparison of attributes of Infrastructure ENUM and ENUM in E.164 (User)

Key issues	Infrastructure ENUM	ENUM in e164.arpa
Who decides to participate in the ENUM scheme?	CSP	Country (Administration) ENUM subscribers
By whom is information required?	CSPs only	Optional information
By whom is information supplied?	CSPs	ENUM subscribers
Who can upload information?	CSP serving the E.164 number	Any single ENUM Registrar per E.164 number
How is information populated?	All E.164 numbers inserted, no opt-in for single subscribers	Opt-in for each ENUM subscriber
Who has access to information?	Intended for CSPs only	Any entity
Is retrieval of information controlled?	Yes	No
Is a domain defined?	No	Yes: e164.arpa

Source: Draft ETSI TR 102 055 (2005-01)

5.3 Public & Private Infrastructure ENUM

The IETF plans to extend the ENUM RFC to include Infrastructure ENUM. Their work assumes that the domain to be used will eventually be the same as that in User ENUM, e164.arpa, but initially will be some other domain, possibly e164i.arpa. This is illustrative of the term Public Infrastructure ENUM. Private Infrastructure ENUM may use any domain, agreed between CSPs. Public Infrastructure ENUM is as yet undefined or agreed whereas Private Infrastructure ENUM is already in use in Europe and the United States.

Since Public Infrastructure ENUM is as yet undefined, we will focus on the Private variant.

5.4 Domain choice for Infrastructure ENUM

The public e164.arpa name space is not considered appropriate for Infrastructure ENUM by many parties, including this Working Group. There are several reasons for this. Firstly, the use of the public e164.arpa domain is constrained by the procedures agreed between ITU, IAB, RIPE NCC and Administrations. CSPs will need to enter E.164 numbers into a name space for Infrastructure ENUM irrespective of whether delegations for country codes have been made in the public e164.arpa tree. Secondly, the public e164.arpa space will normally be governed by the opt-in principle. Numbers would only be entered with the explicit consent of the end user. This is clearly impractical for the operation of a CSP's service.

Finally, it is highly unlikely that the information CSPs publish in the name space for Infrastructure ENUM should be public. It may contain details of border gateways that cannot be reached from the public Internet. Public dissemination of this information could also disclose details about the topology and operation of the CSPs network.

5.5 Functional Model

The ENUM functional and administrative model is based on the separation into three distinct levels: Tier 0, Tier 1, and Tier 2. The levels relevant to a national implementation are Tiers 1 & 2.

In addition to these Tiers, a Validation/Authentication function is required. This function validates the ENUM subscriber's right to use/enter an E.164 number.

Each level is responsible for different functions. The grouping of these functionalities at an operational level will ultimately depend upon the policy and governance decisions made in New Zealand. Whether User ENUM, or a mix of User and Operator/Infrastructure ENUM are deployed, can also directly affect the way these functions are grouped, both in an operational and commercial context.

5.6 Tier 0

The main functions performed at this level are the administration and technical management of the e164.arpa ENUM domain. These functions are implemented by a single international registry containing pointers to the Tier 1 registries.

5.7 Tier 1 Registry

The ENUM Tier 1 Registry functions are management and operation of the ENUM domain corresponding to an E.164 country-code in the country or area identified by that given country code (ccTLD). In New Zealand, this would be .4.6.e164.arpa.The Tier 1 Registry is a national registry containing pointers to the ENUM Tier 2 nameserver providers.

Note: There are several existing USER ENUM implementations that do not use the e164.arpa TLD. Examples are e164.org and enum2go.com.

5.8 Tier 2 Nameserver Provider & Registrar

The main functions performed at the Tier 2 level are the commercial provision of the ENUM functions. These functions are carried out by the ENUM nameserver provider and ENUM Registrar. The nameserver provider and registrar functions can be carried out by the same or separate entities. Depending upon the ENUM model adopted, there may be more than one Tier 2 nameserver provider or Tier 2 Registrars competing in a national implementation.

The ENUM Tier 2 nameserver provider holds the NAPTR records in the format being used by the country concerned. The ENUM Tier 1 Registry needs to point to that nameserver.

The ENUM Registrar acts as an agent to input the ENUM subscriber's ENUM domain name (E.164 number) into the ENUM Tier 1 Registry so that the Registry points to the correct ENUM Tier 2 nameserver provider in DNS. The ENUM Registrar needs to be appointed or recognized by the ENUM Tier 1 Registry.

This tiered architecture approach ensures that two important goals are achieved.

a) The ENUM architecture follows the DNS hierarchy based on delegation as a mechanism to decentralize the control and provide a greater level of scalability and security.
b) Competition and customer choice are properly introduced at the level where ENUM-based services are commercially offered (Tier 2) without interfering with the administration and registry functions performed at the Tier 0 and Tier 1 levels.

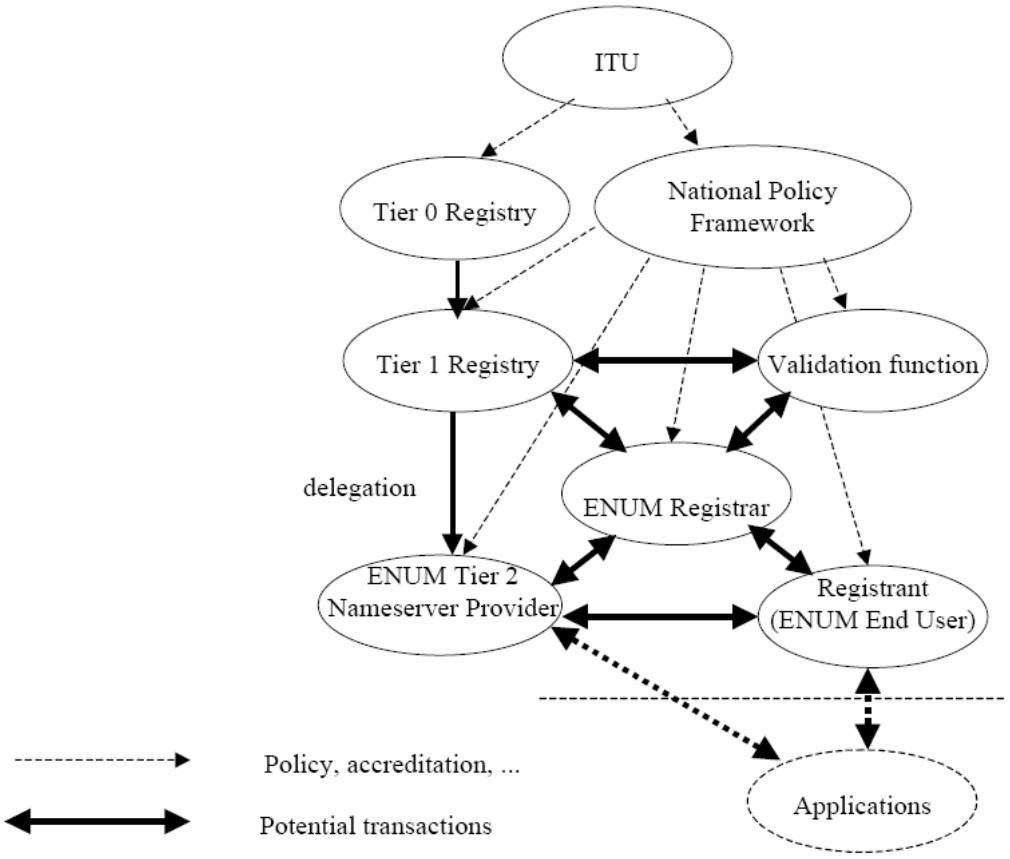


Figure 1: ENUM reference model and functional entities

5.9 Types of Infrastructure ENUM

5.9.1 CSP–internal Infrastructure ENUM

- Uses DNS data that exists and is only accessible within the CSPs non-public IP network (Intranet).
- Can be used in any suitable DNS domain. DNS may be a private namespace or part of the public namespace.

Intended to only be used by a CSP to:

- find users and their services within their own network;
- find the border elements connected to other CSPs, the public Internet and the gateways to the PSTN within their own network;
- access translation databases belonging to the CSP from inside the network using ENUM technology;
- hide the users and infrastructure behind border elements, and give outside CSPs access to these border elements.

5.9.2 CSP–shared Infrastructure ENUM

- DNS data is accessible by all CSPs participating in the system.
- DNS functionality can be within the Internet or a non-public IP network.

- May be in any suitable DNS domain agreed by the participating CSPs. (ETSI recommend that the .arpa is used, although technically this is not mandatory).
- Policy decision over whether the data for the system is in the public DNS and if it is accessible by the public.
- Used by CSPs to reach the border elements of other CSPs.
- NOT intended to be used by end-users and the end-users of other CSPs.
- A given CSP can access more than one Infrastructure ENUM domain and propagate data in different Infrastructure ENUM domains.

Conceptually there is no difference between 2 & 3, only the fact that 2 could be separate disparate 'islands' of Infrastructure ENUM and 3 is a unified approach where all CSPs share a common ENUM infrastructure. This concept could scale nationally or ultimately globally.

5.9.3 Global (or Common) Infrastructure ENUM

- Requires agreement by all participating CSPs to share ONE common Infrastructure ENUM system.
- This system would hold all E.164 numbers hosted by the participating CSPs.
- Can potentially provide global and common connectivity between all CSPs.
- Up-to-date information (under the control of the CSP hosting the E.164 number) is accessible to all CSPs, e.g. ported/ceased numbers.

5.10 Architectural Options

As outlined in Draft ETSI TR 102 055 (2005-01), ***[Note: can we reference in footnote where you can find this?]*** a number of architectures could be adopted by service providers for infrastructure ENUM. An important point to note is that several of these models can be mixed in one group, e.g., different models for different number ranges.

The structure of the Tiers in a CSP-shared Infrastructure ENUM system is a decision for the participating CSPs. *It can be assumed that the Tier 0/Tier 1 roles will be combined.*

Regardless of the model chosen, 2 scenarios exist where an ENUM query does not result in a NAPTR being returned:

a. The serving operator has not entered any information into the system; or
b. Data has been entered, but the particular number is not in service.

Both cases require a different action, case(i) should follow alternate routing procedures, and case(ii) should result in the call being dropped. Participating CSPs should be able to distinguish between the two cases, and act accordingly.

6. SUMMARY OF EXISTING ENUM TRIALS

One of the clearest observations drawn from the respective offshore ENUM trials was the disjointed approach by the various engineering centric organisations toward policy frameworks and governance. From the IETF and ETSI scoping of the initial ENUM standards which formed the basis for the initial ENUM trials, a lack of explanation or definition surrounded what mechanisms actually prove (or demonstrated) a successful ENUM interaction.

As a minimum, customers in either the Internet or telecommunications community should expect to see their URI capable of being mapped to either a PSTN or mobile number of their choosing. After initial trial failures in both Europe and United Kingdom, the UK ENUM taskforce acknowledged this exact point during 2005, after their trial, and have taken significant steps to counter the main privacy weaknesses surrounding User ENUM, and the associated inter-working (required to prove a true ENUM interaction) with a Carrier ENUM infrastructure such as ex-directory services and number portability.

The main lessons learned from offshore trials are as follows:

a. Significant hesitation on the part of numbering bodies, both regulated and unregulated to assign active PSTN number ranges to the ENUM trial – either geographic or non-geographic. Rather a “clean” number range has almost always been assigned;

b. Related to point (a), a complete lack of planning, development or testing around how any eventual billing mechanism will determine, or a means to provide effective non-repudiation of, the CDR exchange between the public User ENUM fabric (subscriber end-point) and Infrastructure ENUM, whether public or private;

c. Related to point (b), no consideration surrounding how the User ENUM mechanisms are validated in either a real time or non-real time manner;

d. Related to point (a), many of the trials either isolated their User ENUM interaction to just a PSTN handoff, hence excluding the widely deployed 2.5/3G mobile environments existing worldwide;

e. Many trials (including Australia currently) repeated similar mistakes in relation to User ENUM trials – where no clear outcomes were set in terms of proving ENUM billing interaction, PSTN to mobile ENUM information exchange, mobile to URI ENUM information exchange etc. The simple fact that existing DNS technology can support User ENUM has been proven already;

f. The mobile handsets used by subscribers provide significant challenges in terms of intuitive usage in the context of ENUM, as the applications don’t yet exist to enable fast dial scenarios. i.e: a subscriber may need to type in an IP address or URI, instead of simply a traditional phone number;

g. The ENUM standards community did not encourage the inclusion of provisions for IMS or next-generation messaging within the initial planning for ENUM, hence very few trials have even attempted to prove a reliable ENUM interaction from (or between) SMS, MMS, IMS, P2T, with an ENUM endpoint such as a URI;

h. Related to point g, the technical constraints commonly referred to as Network Address Translation (NAT) issues clearly exist between SIP based networks

and traditional legacy environments that need to be overcome to prove such concepts;

i. Those countries (Austria and the UK) which allowed disparate User ENUM trees to co-exist, had significant problems constraining and protecting the User ENUM data integrity, both intra-tree at the Tier2 layer, but also interacting with the Tier0/1 infrastructure;

j. The concept that every subscriber in an ENUM trial should have to opt-out, otherwise they will be included in a publicly accessible ENUM database - illustrated significant privacy dangers to the trial participants. The final outcome of most European trials (particularly the UK CRUE initiative) was that the opt-in model is more suitable for an ENUM deployment;

k. In relation to point (j), the fact that a subscriber within a User ENUM mechanism can opt-in with an ENUM endpoint defined as their PSTN service, but they neglected to realise or acknowledge their PSTN service is currently ex-directory;

l. Related to point (k), the ability to opt-out of an ENUM hierarchy is simple enough, but the distributed database model used within most existing User ENUM trees means it will take time for the data replication to catch up, allowing revocation of the published ENUM handle. Meanwhile the record is potentially exposed to the public domain during the time it takes for database replication to catch up;

m. In relation to point (k), no trial provided a significant proof of concept surrounding the secure interaction between an ex-directory database, number portability database, and either a User ENUM tree or Carrier ENUM infrastructure;

n. A common mistake made by most of the User ENUM trials was the lack of administrative protection surrounding the Whois lookup capability of their User ENUM database tree. Existing watermark techniques are commonly used within the Internet community to protect against robots, or whois trawling by identity thieves and spammers. Note: The current Australian trial is unprotected in this manner – http://www.enum.com.au;

o. Furthermore, in relation to both points (j) and (k), the validation at any moment in time of ENUM subscriber trialists was never achieved, and no scope exists currently to achieve this outside of the CRUE initiative in the UK.;

p. None of the offshore ENUM trials included a widespread education campaign for the ENUM user community, either within the corporate or government sectors;

q. Related to point (p), none of the trials directly engaged the application developers to prepare future roadmaps, or participate and contribute to the ENUM trials directly;

r. In relation to point (p), none of the ENUM trials involved large scale interactions with a DNS-SEC hierarchy, or associated authentication mechanism. Without proving this concept, unanswered questions surround the ENUM capability when it comes to military or banking scenarios;

s. In Sweden the government has taken an active role in shaping and planning the ENUM landscape. In doing so, the national agency for post and telecommunications has announced that it will take control of the Tier0/1 management of the ENUM hierarchy including protection of national number plan management, with the Tier2 layer being run by an *"independent ENUM*

service supplier which offers services and portability guarantee's"

t. The Canadian trial concluded with significant questions surrounding the funding mechanism required to pay for the costs of operating the ENUM system, including the management costs of the Tier0/1 layer which interacts with the number plan and portability mechanisms;

u. None of the previous or existing ENUM trials proved the concept of Location Based Service interaction with the ENUM fabric, either at the Tier1 or Tier2 layer;

v. In relation to point (u), the debate regarding how to assign PSTN (or PATS in the UK) number ranges for ENUM delegation still exists. But in Austria, a decision has been reached to assign a specific and dedicated "non geographic" range – to assist with future Location Based Services;

w. In relation to point (v), no proof of concept occurred within any of the previous ENUM trials surrounding lawful intercept capability, including but not limited to proposed capture points for Tier0/1 and Tier2/3, or the underlying architecture required to facilitate secure transmission of this requirement on behalf of government agencies;

x. In relation to the ENUM trials proving the concept of a reliable Personal User Agent (PUA), none of the trials implemented concurrent (or dedicated) IPv6 for testing – even though the military organisations and other critical infrastructure providers and consumers have stipulated that all of these organisations must be IPv6 native by the end of 2007;

y. According to one of the few countries using ENUM commercially, ENUM cannot be sold, only services that use ENUM. Neither customers nor the application development community yet understand ENUM; and

z. Private Infrastructure ENUM is in commercial use in both Europe and the United States. There are multiple vendors providing solutions enabling Private Infrastructure ENUM. Such implementations do not use a public or single tree (root) DNS infrastructure and many do not use any DNS infrastructure to deliver ENUM. Rather they use existing datasets contained in databases such as those used for number portability of mobile specific data such as IMSI. And their use is restricted to a defined user community generally trusted service providers thus avoiding privacy, accreditation, validation and other issues.

7. STANDARDS BODIES UPDATE

7.1 ENUM WG (Overview of IETF & ETSI)

The initial standards were devised by technologists and, as such, the original ENUM RFC documents demonstrated little appreciation of, or concern about, the implications of ENUM on the global E.164 numbering mechanism, and eventual subscriber privacy. The original RFC2916 document contains neither the word 'privacy', nor any other reference to the proposal's social implications. Policy-wise:

- the ENUM WG home-page and charter provide no evidence whatsoever of any recognition of, or interest in, the implications of the initiative;
- the consolidated collection of reference materials at NGI (2001-) contains no heading that acknowledges that serious privacy concerns have been expressed about the proposal. Considerable amounts of technical criticism have also been leveled at it;
- the RFC2916's author, WG co-chair Patrick Fältström, has made many presentations around the world socialising the idea. The versions of his slide-set seen to late 2002, e.g. at http://www.ripe.net/ripe/meetings/archive/ripe-41/presentations/dns-enum/, contain no acknowledgment whatsoever of the existence of social implications, or of uproar in the privacy advocacy community.

In recent work undertaken by ETSI in late 2005, serious attempts have been made to wrap some policy around the security of existing and future telephony services so as to protect the subscriber identity, and more specifically to protect children from IP related abuse. At this stage, it seems that none of the major advocacy bodies have had any significant interaction with the IETF WG though. This includes the primary organizations in the area, Electronic Privacy Information Center, Center for Democracy and Technology, and Privacy International.

The Discussion Paper issued by the Australian Communications Authority (ACA) in September 2002[1] was a little more circumspect, but remained vague as to countering the technical constraints around privacy protection. The document expressly recognised that threats to privacy were embodied in the ENUM RFC2916, and the questions namely surrounded policy issues, risks to the public, and questioned opt-in scenarios in relation to security and privacy. It is unclear whether the ACA have taken on board the criticisms and recommendations in this paper, and the submissions of the APF and EFA – but judging by the very public nature of the existing ACA trial in Australia it seems not.

The FCC, in the conditions it applied to the US ENUM trial that began in February 2006, ensured that privacy issues and social implications were considered fully.

In a belated acknowledgement that serious privacy issues arise from the ENUM proposal, Shockey wrote an Internet Draft, which was published in late 2002[2]. This repeats the belief that "administration, management and control of the zones and

[1] "Implementation of ENUM in Australia", discussion paper released by the ACA available on www.acma.gov.au (the ACA and the Australian Broadcasting Authority merged to become the Australian Communications and Media Authority (ACMA)).

[2] "Privacy and Security Considerations in ENUM" Richard Shockey, IETF ENUM Working Group, Internet Draft, document: draft-ietf-enum-privacy-security-01.txt, July 2003.

administrative portions of the E.164 plan are nation-state issues". It canvasses ways in which identification data could be obscured, but fails to reach any conclusion; and it fails to propose any changes to the draft standards: "The concept of a Service Resolution Service has not been defined in the IETF, however it is within the realm of technical possibility".

7.2 Infrastructure ENUM Standards Activities (GSM)

THE GSM Association (GSMA) has proposed an infrastructure ENUM solution based on the use of the GSM Global Roaming Exchange (GRX) backbone network, using the ENUM TLD e164enum.net. There are already trials being run in GSMA for testing of GSMA's Carrier/Operator ENUM tree.

> ***Quotes from Nick Russell, Vodafone representative on GSMA ENUM WP:***
> ***"Some nations are supporting User/Public ENUM (which uses the e164.arpa tree), such as Austria and very soon, the USA. However, these nations are learning that there simply isn't a market need for User/Public ENUM; mainly because people don't want to put their e-mail addresses into a globally accessible database…as they're already fed up with the spam that they get and don't want to provide for more. Vodafone is supporting and driving Carrier ENUM on the GRX, through participation in the likes of GSMA IREG Packet ENUM adhoc and also the GSMA IREG GRX Evolution adhoc."***

Carrier ENUM and Operator ENUM are also two of the same, however there is no one Carrier/Operator ENUM; there are numerous private implementations (such as the one that will be set-up on the private - for MNOs - GRX network) and there is work just kicking off in the IETF to provide for a Carrier/Operator ENUM "somewhere" on the Internet (the tree structure hasn't been decided yet!).

The GSMA are proposing the following architecture to blend together Infrastructure and User ENUM implementations:

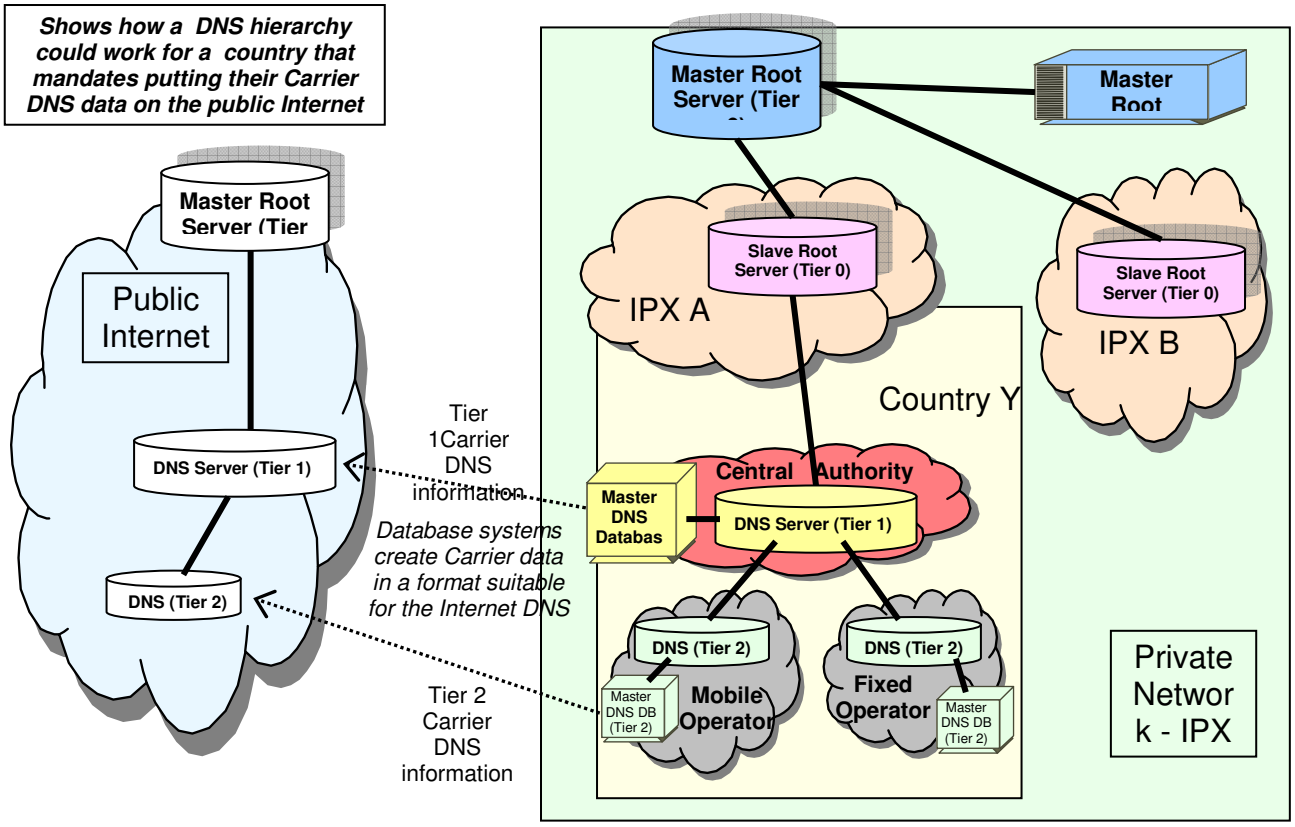


Figure 2: GSM-A Proposed Conceptual Architecture

Privacy and security concerns in this architecture are addressed by:

- Putting Carrier DNS on a private controlled-access network; completely separate from the public Internet;
- In those countries that require their telecom information to be publicly available on the Internet, the telecom information is made available in the Carrier DNS on both the Internet and the private network;
- The controlled-access network is the IPX network (enhanced GRX);
- Any organisation that wishes to connect to the IPX can do so provided that they adhere to the contractual terms of their chosen IPX provider;
- Competition between IPX providers;
- Other private telecom networks (e.g. CDMA networks' CRX) could be connected to the IPX - an area for further study;
- The SIP/IMS calls, MMS messages etc run over the same IP network as the DNS traffic; and
- Existing number portability arrangements can be integrated into the ENUM solution in "Carrier" DNS as desired. Preferred design will vary by country.

7.3 Infrastructure ENUM Standards Activities (ETSI)

ETSI is coordinating ENUM activities within Europe. Their aim is to provide a basic set of principles that should be adhered to in order to maximise potential benefits from publicly available ENUM implementations within Europe.

European principles from ETSI:

- E.164 integrity must be maintained;
- Compliance with Data Protection Directives;
- Adherence to ITU Recommendations and IETF Specifications;
- Compliance with national regulatory requirements;
- Must facilitate a competitive environment;
- Must be user 'opt in';
- Existing network functions must not be compromised e.g. number portability, carrier selection;
- Network hijacking to facilitate bypass;
- Provisioning based on false information by users;
- Authentication and validation requirements;
- Abuse of data stored;
- Regulatory requirements;
- Alternative ENUM implementations;
- Additional ETSI work underway;
- Infrastructure ENUM; and
    - considers ENUM implementation scenarios
    - raises new issues
    - no opt-in for routing
    - different part of namespace?
- ENUM Privacy
    - Looking to provide guidelines for ENUM.

7.4 UK ETG (ENUM Trial Group)

7.4.1 CRUE

In an environment where both User and Infrastructure/Carrier ENUM exist, the ability to provide rigorous validation of an E.164 number holder's "right to use" is potentially made easier by the participation of the TSPs. This comes about by the fact that the TSPs are able to assist the non-TSP entities, (Registrars run by ISPs), in providing validation services.

In late 2005, an initiative called CRUE (Carrier Registration in User ENUM) was proposed.

In the CRUE model, Carriers "opt-in" to input their assigned blocks of E.164 numbers into the Tier 1 Registry. CRUE also provides a method of self policing participants within the ENUM environment, through codes of practice.

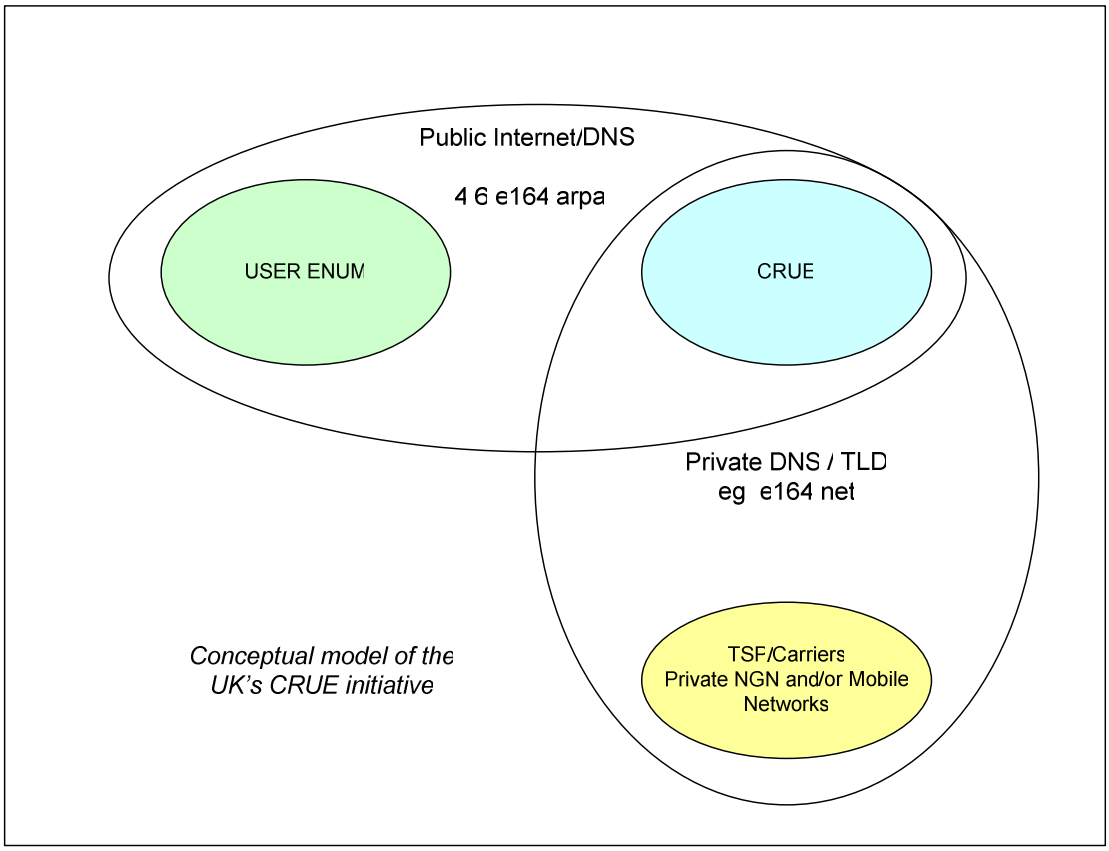


Figure 3: CRUE conceptual architecture diagram

8. REGULATORY IMPACT

8.1 LMNP Code & Anti-Spam Code

A full review of current regulatory codes to ascertain the potential impact of ENUM has yet to be undertaken. Suffice to say, there are likely to be a large number of issues to be addressed with regard to user privacy, data integrity, user authentication and the like. It is recommended that a full review of current TCF codes be undertaken at a subsequent phase, when an ENUM trial is planned and undertaken.

There is the potential for any future ENUM implementation to impact on the current planned New Zealand LMNP implementation. In particular, ENUM records for a given subscriber may need to be updated with new end-points in the situation where the called party has ported their number from one service provider to another. There is the view within some of the offshore ENUM working groups that ENUM could eventually supersede current national number portability regimes.

User / Public ENUM has a significant number of issues associated with user privacy and data integrity. There is a significant potential for spam issues in the event that user ENUM is enabled.

9. MAJOR ISSUES

9.1 Wider Political Considerations

The ENUM design also gives rise to a number of serious concerns in the areas of:

- national infrastructure security;
- +64 national number plan integrity;
- *.nz country level domain name integrity;
- Root (F) name server security and protection; and
- E164.arpa ENUM delegation and control.

The ENUM Working Party has not explored these issues in detail. However, as a minor example, an overseas interest, Instra Corporation, based in Australia, has registered www.e164.co.nz. That domain is the usual one that would be used for the public ENUM tree in New Zealand.

This leads into a more serious example of a political issue, that of national number plan integrity. Without proper process and control +64 ENUM numbers could be provided outside New Zealand jurisdiction by New Zealand and offshore companies making privacy issues and enforcement extremely difficult.

9.2 Known Subscriber Issues

- A silent listing telephone-number can currently be reached without being published; but under the ENUM proposal it could not be.
- Opt-out is totally unacceptable. It is essential that opt-in be entrenched into the scheme. I.e. customers must choose to be part of the service rather than be included then opt-out.
- Operation of the scheme must not discriminate against consumers on the basis of their privacy choices. The current design appears unable to avoid this completely unacceptable outcome.
- The implications of opt-in and silent listing are far wider than in today's numbering environment. Today, if a silent listing or PSTN number is compromised or if a customer has issues with their number it is quite simple to change. Under ENUM, once a customer has opted in, it is extremely difficult to opt-out. Changing a number will not protect the customer, only changing their top level ENUM identifier (URI). This has wide implications for privacy, identity protection and the validation and security infrastructure necessary to support ENUM.

In order to identify future ENUM implications, it is first necessary to acknowledge the inroads that have already been made into the freedoms of citizens and consumers by the expansion of data surveillance methods, including identification and identity authentication, and particularly the location and tracking technologies in a mobile phone context.

In 1999, the USA commenced an initiative to allow their rapid response when a subscriber contacted an emergency service number like (111 or 000), and was no longer able to communicate in the event of serious injury. So a subscriber's handsets are now trackable to within a few hundred metres whether GPS exists or

not. Since the events of 9/11, similar initiatives are now being driven by an alliance of national security, law enforcement, and corporate marketing interests within each country or jurisdiction under the ITU specification embodied in IMT-2000[3], and described in Recommendation ITU-R M.816. In Australia, they are being developed by an industry association, the Australian Communications Industry Forum (ACIF), under the code-name Mobile Origin Location Indication (MOLI).

In relation to ENUM, the underlying ability to track and monitor IP addresses remains. Even in a mobile IP context, the fact that at some point in time a particular IP address was assigned (or bound) to a device provides the inherent ability to track it. This is where the area becomes a little chaotic, as Internet vandals and criminal minds can subsequently use this assumption to their advantage. The challenge from an operator's perspective will not necessarily be policing, but implementing counter-measures so as to avoid IP related fraud such as spoofing, identity theft, malicious and offensive content, or service disrupting Denial of Service spawned from the future ENUM registries, or underlying DNS fabric.

In New Zealand, the industry has only recently implemented the anti spam type codes and an internet related email have been busily taking advantage of the increased public concerns about terrorism by increasing the ease with which national security and law enforcement agencies can gain access to call records, the content of conversations and message transmissions, and the location data contained within telecommunications systems. At this stage, the process has successfully avoided any significant public participation or even public exposure which from an operator's perspective, if legislated, could potentially translate into:

a) ENUM creating a unique individual identifier, which facilitates the location and tracking of subscribers by marketers, spammers, and governments;
b) Data about Internet-connected devices being public, but not information about people's locations;
c) Privacy protection features becoming seriously inadequate, and the mooted `Service Resolution Service', to support pseudonymity, is as yet undefined; and
d) Existing privacy laws becoming seriously deficient, and significant enhancements would be essential.

Although the ENUM trials have not yet attracted significant market traction as a result of poor developer and subscriber education, evolving technical implementations, and many industry skeptics hypothesize that ENUM will never attract much interest from retail consumers because the primary VoIP driver still appears to be the intended cost savings of large corporations who can potentially leverage existing data infrastructure and route voice traffic over the Internet rather than via a traditional telecommunications operator.

[3] International Mobile Telecommunications-2000 (IMT-2000) is the global standard for third generaion (3G) wireless communications, defined by a set of interdependent ITU Recommendations.

10. MAJOR RISKS

10.1 Service Integrity

Several previous contributions have suggested that certain types of ENUM registrations might compromise the service integrity of E.164 numbers, in particular non-geographic numbers. This section attempts at least an operational definition of service integrity, provides some examples where service integrity might be thought to be compromised, and suggests some of the ways in which such violations of integrity might be prevented.

"Service integrity" in this context means the expectations about treatment and charging that exist when the number is dialed in today's PSTN environment. These expectations are usually discussed as being based on the service associated with a particular non-geographic NPA or special access code, e.g., the 8YY toll-free codes. The expectation is that calls to toll-free numbers are indeed free.

It is possible to extend the concept of service integrity beyond non-geographic numbers. If dialing a number that a user knows to be within the normal local calling area of his or her present location results in toll charges, has the service integrity of the geographic number been violated?

If dialing a number that would normally result in toll charges, does not, has service integrity been violated? If it has, should we care?

Are there any violations of service integrity of concern that do not involve charging the user more than they expected under a PSTN regime? For example, if a number assignee associates an email address with the E.164 number, is this a matter of concern?

10.2 Example Violations of Service Integrity

10.2.1 Toll-Free number points to a telephony (tel) URI associated with a call resulting in toll charges.

The legitimate assignee of a toll-free number could have provisioned a NAPTR record that would result in a telephony URI that, if utilized by the originating client could result in a PSTN call for which toll charges would apply. Consider several variants of this case. In the first, the client belonging to the originator directly makes the ENUM query and acts on the result, placing the call either directly on a PSTN line it controls or through an IP hop-off carrier. A principle articulated in the SG A Ad Hoc report is that originators of communications are neither obligated to query ENUM nor to make use of the results of a query if they choose to make one. If well designed client software showed the user the number that would be contacted based on the returned NAPTR record and asked whether or not to proceed, would service integrity be violated? In a second variant, the ENUM query is performed not by an ENUM-enabled originating client but by a carrier serving the caller who may be using a basic telephone. In this case we (and the regulators) would probably look askance on a carrier that completed the call and billed the caller toll charges without notification and the option to decline the call.

10.2.2 Geographic number local to the caller location points to a tel URI associated with an international call.

The legitimate assignee of a geographic number could have provisioned a NAPTR record that would result in a tel URI that, if utilized by the originating client could result in a PSTN international call. This might be done quite innocently with intent like call forwarding. Has service integrity been violated? Is this so only in the case where the caller is not informed of the redirection and offered the opportunity to cancel the call? How does responsibility vary with whether the ENUM query is done by the originating client or a carrier?

10.2.3 Maintaining Service Integrity

Because service integrity issues are not limited to certain number classes, they cannot be resolved by disallowing ENUM registration of domains corresponding to certain number types. Two sorts of remedies are conceivable. First, provisioning of resource records that could be expected to violate service expectations might be disallowed. This is not likely, however, to prove feasible, short of disallowing all telephony URIs. Too much knowledge about PSTN rating on the part would be required to determine what NAPTRs might lead to violation of the integrity of different numbers to implement a lesser restriction, and, given that registrants may serve as their own Tier 2s, such restrictions, even if appropriate, could not always be enforced prospectively.

Second, ENUM enabled client design standards could require confirmation by the user when a PSTN call to a number other than that queried is indicated as the result of an ENUM query, and carriers could be required (if they are not already) to not charge extra for ENUM based call redirections of which the caller has not been informed.

10.3 Validation

The validation of the relation between the E.164 number and the end user to which it is assigned as well as the status of an E.164 number is crucial in ENUM.

Validation is needed during the initial entering of a number in ENUM. Validation is also needed after a number has been entered, to ensure that the numbers in ENUM remain assigned.

One of the goals in the development of an implementation for the administrative processes in ENUM may be to have a validation process that is simple while, at the same time, discourages fraud and unauthorized creation or transfer of services.

Depending on the national telecommunications environment, the simplicity or complexity of the validation process may be an important criterion in the assessment of different implementation options.

The appropriate method for validating the relationship between an E.164 number and a telephony subscriber may vary from country to country depending on whether number assignment validation procedures exist in other contexts (such as for requests for porting of numbers), the weight of any legal provisions for dealing with fraudulent requests for action in relation to ENUM data, and the range of entities which hold information on number assignments.

The following options are offered for consideration:

- The registrar relies for validation on a third party entity that holds information on the relation between an E.164 number and the end user to which it is assigned. Depending on the national telecommunications environment, this entity may be the Telephone Service Provider (TSP) that provides the telephony service for the number involved, or the NNPA in the case of numbers that are assigned directly to end users, or directory database operators. In New Zealand's case, the NAD does not assign number allocations to end users, but to active NAD members, who in turn assign individual number ranges to end-users;
- It is worth noting that, where this third party entity is a telephone service provider, it may be necessary for the registrar to have a method available for determining which is the relevant TSP to contact. Such a method may need to take special account of any ability of end users to port numbers from one service provider to another; and
- The registrar relies for validation on receiving an appropriate standard of documentary evidence from an ENUM registrant demonstrating that the end user has been assigned the E.164 number. Suitable documentary evidence might be a letter or digital certificate from the body that assigned the number to the end user that substantiates the assignment, or a bill from a TSP that demonstrates that a telephone service is supplied in connection with the number. It may be necessary to take account of the age of possible types of documentation reducing their value.

These two options are illustrated below:

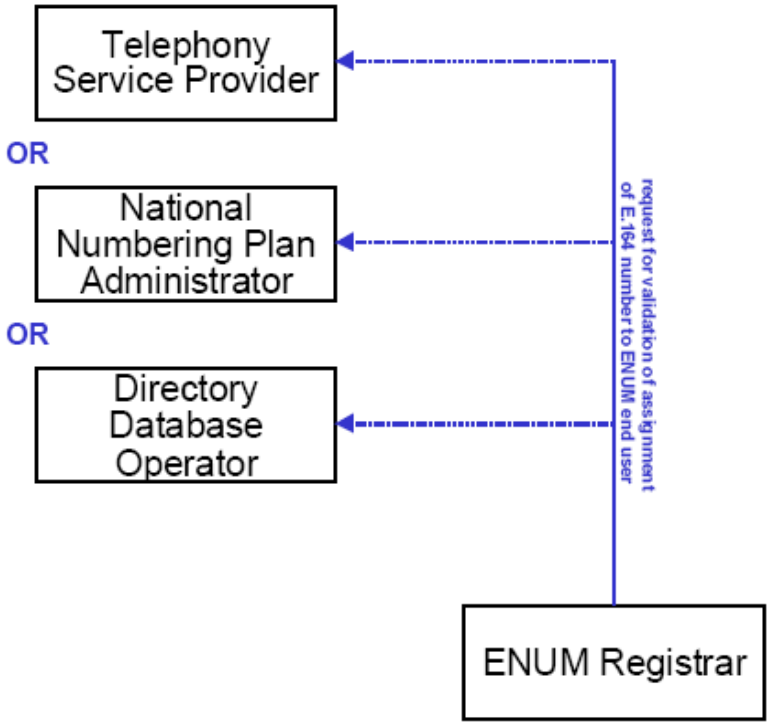


Figure 4: Validation of assignment via third party entity

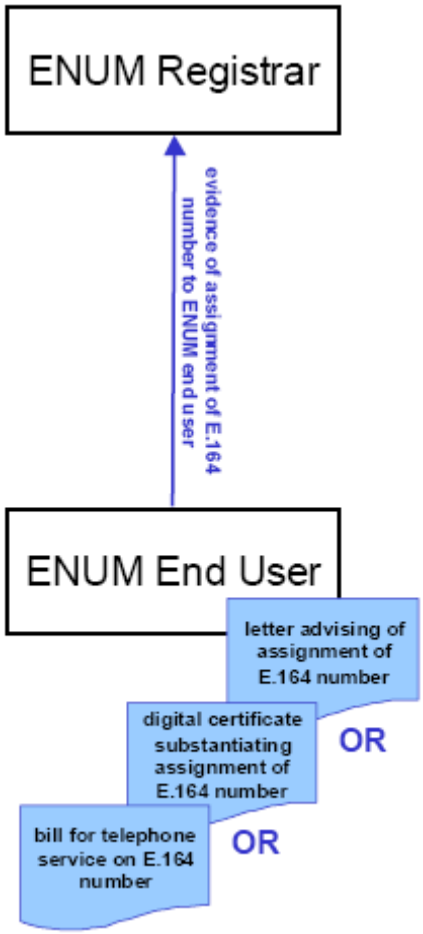


Figure 5: Validation of assignment via documentary evidence

10.4 Removal of E.164 Numbers

In the case where an E.164 number is withdrawn, the number has to be removed from ENUM. In general, it is not always possible to rely on the ENUM registrant for the triggering of this removal process. Several ways may be available to ensure that numbers that are no longer assigned are removed from ENUM:

- One option may be for the entity that has the information on the relation between an E.164 number and the end user to trigger the removal process. This entity may be the telephone service provider that provides the telephony service for the number involved, the service provider in the case of numbers that are assigned directly to end users, or directory database operators.
- Another option may be to periodically check the assignment of the individual E.164 numbers in ENUM through repeating the processes used for the initial number validation process. When determining the frequency of revalidation the ageing period used between ceasing a number and reassigning it should be considered. In principle the revalidation period should be less than the ageing period.

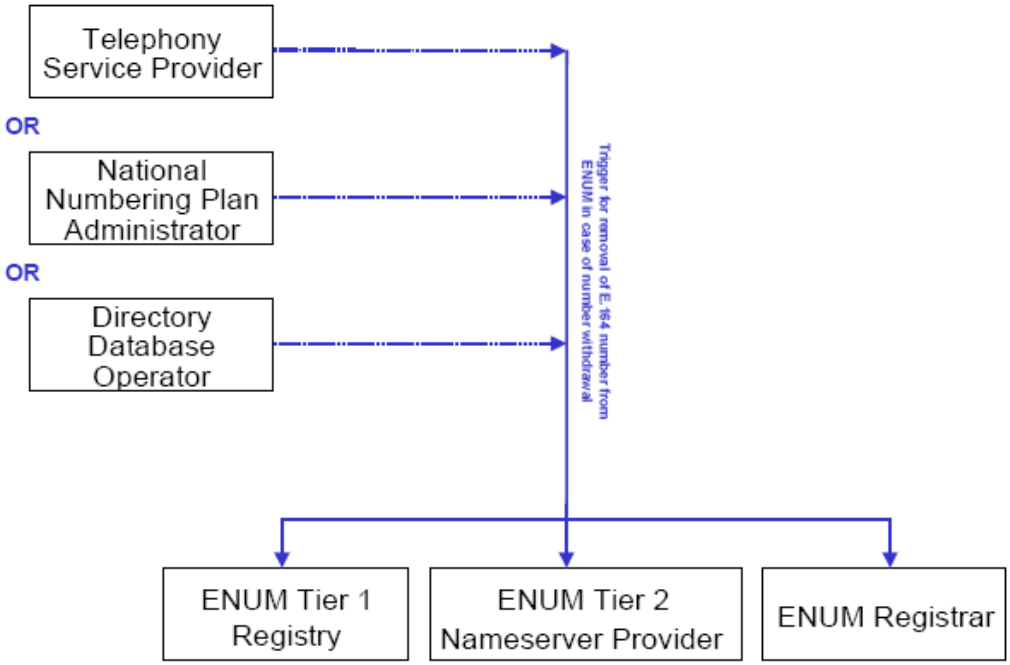


Figure 6: Triggering of the removal process by third party entity

Because it is unlikely that any method of validation can be perfect, ENUM administrative processes should include back-out procedures that can be quickly invoked in the case that an action in relation to ENUM data that corresponds to an E.164 number is deliberately or inadvertently taken by a person who is not authorized by the relevant end user.

10.5 Authentication

In a User ENUM environment, by the very nature of its “opt-in” philosophy, there is no concept of “trusted parties”, and as such, every transaction is required to be authenticated. In practice, depending upon the participating Tier 2 entities operating procedures, this may or may not happen. This applies to both the Registrar and the

nameserver providers. Any lack of rigor in this area can, and will, lead to the compromising of the ENUM subscriber's privacy through the use of common internet abuse techniques.

Unlike User ENUM, all the participants in a Private Infrastructure ENUM environment are considered to be trusted parties, so it may not be necessary to implement any authentication (validation) process when a communications provider wishes to populate a given number or number range. This is particularly the case where the group is a series of co-operating communications providers.

However, the concept of Infrastructure ENUM will expand so that the participants are merely communications providers who have agreed that it would be mutually beneficial to share information via ENUM, but who, at a commercial level, are competitors. In this situation, it will be necessary to address whether some form of authentication is appropriate, e.g. to prevent situations where call hijacking could occur.

The likelihood is that in this situation a mechanism will be required to confirm that a given communications provider has been assigned a given number or number range. However for Private Infrastructure ENUM it is assumed that this process could be very basic when compared to that for user-ENUM, and also that there will not be any necessity to confirm the identity of the service provider.

It may be necessary to safeguard the integrity of DNS data from attacks on the DNS infrastructure. These threats include the accidental or deliberate publication of bogus DNS data, DNS spoofing attacks and tampering with DNS responses to hijack traffic. Possible defensive measures could include the use of Secure VPNs or DNS security protocols such as transaction signatures and secure DNS.

Various methods of authentication have been talked about for use within ENUM. The most popular method is the use of "validation tokens".

Currently there is a "work in progress" by the IETF (ENUM Validation Token Format Definition - draft-ietf-enum-validation-token-02) which outlines how a token based validation system might work. By the very nature of the digital signature discussed in this draft, the 'authenticity' of validation information is confirmed. The use of tokens also provides a method of auditing the validation process (non-repudiation).

10.6 Accreditation

The question of accreditation of participating roles in ENUM has been widely discussed in many trial reports.

Accreditation is seen as a method of ensuring that organizations participating in ENUM meet a minimum standard of operating practices set down by the industry. The main advantage from an accreditation regime is the inherent level of trust assumed between the parties.

The existence of any accreditation scheme would also assume that there was a suitable mechanism in place which would allow the effective enforceability of the relevant regulatory and legal obligations on each role.

Appendix J of this report contains Annex E from the UK ENUM Trial Group (UKETG) Report May 2004.

This document outlines the various options for accreditation models, and makes recommendations as to what considerations must be for the production ENUM environment.

These recommendations can be summarised as:

- There is a clear need for an accreditation process for key roles in ENUM;
- Although there is no recommendation of which accreditation model should be adopted, there is a need for a complaints process by which alleged breaches can be dealt with, and appropriate sanctions made;
- The conduct, procedures and practices of the Tier 1 Registry will be covered by a contract with the body controlling ENUM;
- Tier 2 nameserver providers are not required to be accredited due to their "vanilla DNS" role in ENUM;
- Registrars and authentication agencies (Validation Entity) were identified as requiring accreditation;
- Registrars could be accredited via self-certification. The Tier 1 Registry will only accept registrations from accredited registrars; and
- An appropriate policy group under the TCF Board or the EISG would be best placed to set the accreditation process/criteria and also manage the complaints process.

It should be noted that the need for an accreditation scheme exists mainly in the Public ENUM space where the ability to participate is open (untrusted). In a Private Carrier/ Infrastructure ENUM environment, an implicit level of trust exists due to its co-operative nature. The mechanisms required for an accreditation scheme already exist within the carrier (TCF) world, namely a common body to form codes of practice.

11. ENUM INTEROPERABILITY

As has been discovered during offshore trials, ENUM itself cannot be sold. However, the space for applications that use ENUM is limited only by the creativity of the market players. Obviously, since this may result in commercial gain, it is likely that the participants in the New Zealand ENUM pilot might keep their applications ideas to themselves. The list below gives an idea of the application space so that infrastructure (wg ENUM4) and processes (wg ENUM2) are designed to support rather than limit the development of applications.

The ENUM1 working group has discussed applications and services structured as follows:

- Applications that aim at making operators and service providers more effective; and
- Applications that aim at making an end user – residential or enterprise – more effective. These can be further grouped into:
    - information services
    - one-to-one services
    - advanced services
    - maintenance services.

In this context the terms applications and services are used interchangeably. We understand that the Internet culture prefers the term 'application' whereas the telephony culture prefers the term 'services'.

The term 'effective' is used as a two dimensional concept, where one dimension is customer value and the other productivity. An enterprise can be effective by maximising the value its services brings to the customers or by maximising productivity i.e. the cost of producing a unit of service. In practice an enterprise tries to strike a balance between the two dimensions in order to be maximally competitive.

ENUM based services/applications can be targeted to focus on productivity for instance by short circuit or circumvent present remuneration rules. But these are short term solutions subject to adaptation and countermeasures by operators. Although these services certainly have the value of being a catalyst of market developments, the main value of ENUM is to constitute a platform for new functionality that can improve the customer value dimension.

It is presently difficult to predict the value of ENUM-based applications for consumers and even more so to foresee all implications for the consumers. In general it is probably good for the customer, be it enterprise or residential, that the telephone networks and Internet is integrated.

Also from an operator's perspective it can be good to offer customers unlimited call forwarding between telephone networks and Internet. Already today it is possible to within operators' networks transit calls and port telephone number, but the option to route one's telephone number to, for instance, Internet applications is missing.

The problem to link together or integrate Internet and telephone networks is that they are designed and owned in different ways. Also the technical solution of communication is significantly different.

There are several hazards with a possible implementation of fragmented User ENUM trees. One is that the operators lose control over all assigned numbers from the number plan. An unlimited right of forwarding calls from E.164 numbers to, for instance, Internet applications that the customer can control increases the probability of disturbances and faults in the traffic distribution, which in its turn leads to a lesser degree of security in telecommunications. If ENUM is implemented there must exist an unconditional right for operators to, from radio- and tele-technical reasons, deny registration of certain connections between E.164 numbers and Internet based addresses.

Another hazard is that the operators, as was the case when implementing number portability, has to make investments that are not compensated by revenue increases. If so it is more the case of introducing new costs on the operators. It is naturally premature to evaluate mobile number portability, but to date the utility for users is considerably less than their direct and indirect costs.

ENUM may also lead to some traffic being routed out of the operator`s network, which diminishes revenue and thus the incitement for operators to invest in future mobile technology.

If ENUM is to be implemented in New Zealand, one should as far as possible design a system similar to that for number portability. For that system the operators have already made major investments that should to a maximum extent be reused or built upon. Furthermore the control of the functionality (Tier 2) must reside with the operators. A solitary New Zealand implementation must however be avoided.

11.1 One to One Services

This group of services provides for a session between one application and one other via an E.164 telephone number. This includes a large set of potential services whose value can only be determined by the creativity of the designer. Services can be of several kinds.

11.2 Traditional Basic Calls including SIP Based Services.

Name	Description
Fixed to fixed PSTN telephone	The value of ENUM to such a service is a little unclear. Perhaps it could be of value as a component in a broader Universal Personal Telecommunications Service (UPT), or as a means of using Internet as a less expensive transit facility between originator and terminator operator PSTNs. Includes fax to fax.
PSTN to PLMN and vice versa	Same considerations as above. PLMN can be NMT, GSM, UMTS and other 3G or other cellular network operators. Includes fax to fax.
PLMN to PLMN	Regarding value see PSTN to PLMN above.
International calls	Including all of the above varieties of services.
PSTN or PLMN to services	Connection to premium and freephone calls via an E.164 number.

SIP telephone to SIP telephone	The “telephone” can be a dedicated IP-telephone or a software based telephony function.
SIP telephone to PSTN, PLMN and vice versa	Calls from a hardware or soft IP telephone to a fixed telephone number (geographical, service or international) or a PLMN number and vice versa.

11.3 Converted Application Services

This set of services requires a more complex and ‘intelligent’ conversion (and implementation of functions) between the calling and called party terminals and applications.

Name	**Description/Commentary**
SIP-to-SIP	This is a group of potential services including voice, video, chat, interactive games and virtual reality in the calling party’s end to the same variety of functions in the called party’s end.
SIP-to-PSTN or PLMN and vice versa	Calls from all SIP based sessions (voice, video, chat, interactive games and virtual reality) to PSTN (geographical, service, international calls) or PLMN and vice versa
E-Mail to fax	Converting an e-mail to a fax message
Electronic document to fax	
Fax conversions	In the near future it might be possible to convert a fax to e-mail, electronic document, SMS or even a voice message.

There are definitely interesting services within this scenario. ENUM can be used for least cost routing, and if there is a e.g. UPT service for a specific E.164-number directing the call to a number without Internet address there will most probably be PSTN-PSTN calls guided by SIP-services triggered by ENUM.

However, there are problems in this area. If the originating number is e.g. PSTN calling a number for which there is an ENUM-service defining e.g. an UPT-pattern. How does one make sure that the ENUM-service is actually called? The only way we can see is that the customer makes the agreement regarding the ENUM-service with the operator responsible for the number including a deal that any PSTN-call to this number must be checked for ENUM-service. There is a possibility that the ENUM check is called from the customer equipment behind the number, but in that case the direction of the call to another PSTN-number (outside the PABX-domain) will be a new call with new charging.

11.4 Extended One-to-One Services

These are one-to-one services that extend more or less traditional 'Basic Calls' to new areas. Examples are:

Name	Description/Commentary
E-mail to E-Mail	This is e-mail to e-mail via an E.164 number. The E.164 number then serves as a means of finding an e-mail-address.
E-mail to SMS/MMS and vice versa	Using the E.164 number as a means of finding an SMS or MMS number.
http-to-http	Using the E.164 number to find a home page
Voice to e-mail	Sending a voice message over e-mail and vice versa

11.5 Advanced Services

We use the term advanced services when services are making an intelligent choice between different alternatives. Often, advanced services builds upon the one-to-one services above.

Name	Description/Commentary
Extended messaging	An application which looks for alternative ways of sending a message and makes an intelligent choice between them. For example the calling party is trying to send an e-mail to a recipient via the recipients E.164 number. If the recipient has an e-mail address the message is sent to that. In the absence of an e-mail address the message could be sent to SMS. And vice versa.
Extended Universal Personal Telecommunications number, UPT	In traditional UPT the user informs the system at which telephone number he can be reached in a particular point in time. Perhaps even a role based number selection. With ENUM this can be extended from telephone numbers to various Internet services (for instance E-mail) and SMS/MMS.
Extended unified messaging	The above kinds of services can be extended to find a proper match of communication channels by involving also the calling party E.164 number (A-number) in an ENUM look-up.
E-meetings-/conferences	ENUM can bring elegant solutions to electronic meetings and conferences by involving parties over various communications channels in a user friendly way (PSTN, PLMN, SIP)
MMS handling	ENUM can be used to verify that a recipient has a means of receiving MMS messages. Reception may not be limited to the mobile telephone but can be reached from a web address and perhaps e-mail.
Call center support	A-number and B-number can be used to locate a homepage thus enabling an intelligent telephone dialogue supported by web information, forms etc.

Simple and secure Mobile Internet Access	Accessing Internet services from a mobile telephone could be cumbersome – connect to GPRS operator`s network, browse to the service and log into it. ENUM could simplify this while maintaining or even increasing security for instance by looking up an LDAP URI that points to originators public key.
A-number based services	A potentially useful property is that PSTN A-number (calling party number) can be retained in the Internet world and used as an identifier to the caller for remuneration both in a fixed and mobile Internet world. The information can also be used to block users that is not wanted because of abuse, no payment etc.

11.6 Maintenance services

Name	Description/Commentary
URI management	Enables an end-user to add, change or delete URI information
Ext UPT management	An extended UPT service as described above requires a set of services whereby an end user dynamically from different devices can modify his profile on how to be reached
Ext Unified messaging	An extended Unified Messaging Service is likely to require a set of tools whereby an end user can view and manage the database of incoming messages.

11.7 Services – a general model

It might be useful in considering future ENUM based services in the perspective of a traditional IN model. In this model A-number and B-number together with parameters (such as date and time) and sometimes additional user data is used to calculate a C-number or the final destination of a call. With ENUM A-, B- and C-number is not restricted only to E.164 numbers but includes the entire list of addresses that has been extracted by the ENUM procedure.

11.8 Remuneration

ENUM in its current form can potentially be used to circumvent existing tariffing procedures surrounding the interconnect point, since the Internet can be used for access, originating, transit, terminating and associated services and combinations thereof. The option of using ENUM for least cost routing could also be a utility for operators.

11.9 Potential list of Originators and Terminators

Following is an attempt at making a list of all potential originators (Corresponding to A-number) and all potential terminators (Corresponding to B-numbers). The list is grouped by basic underpinning network (architectures) and the main entry is the type of application or terminal device.

The idea is that a user, calling party (identified by his E.164-number – A-number) is using one of the originating applications/terminals below and initiates a session with another user or application/terminal, called party (identified by its E.164-number).

Depending on the associated ENUM list retrieved by the called party B-number and possibly the associated A-number list different capabilities may be envisaged as illustrated below. Of course all combinations of originator designator may not be possible. The terminator, also associated with an E.164, will have a subset of the list below associated by the ENUM process.

The interesting questions will then be what potential combinations of originators and designators will be possible and relevant from a technical, administrative or commercial standpoint, and how they can be classified. One of the classifications is the “traditional” communication in some sense, i.e. PSTN/ISDN/Mobile telephone to PSTN/ISDN/PLMN telephone calls. Another set may be “extended”, i.e. IP telephone to PSTN/ISDN/PLMN or even e-mail to e-mail. A third set may be referred to as converted, i.e. e-mail to SMS.

When bridging between the PSTN/ISDN/PLMNGSM and the Internet domains, it is assumed that ENUM can be used in the PSTN/ISDN/PLMN gateways as a means to facilitate the interworking with the Internet domain.

Consequently, the following list of potential originating/terminating can be envisaged, in some cases in the near term in some cases subsequent to further standardisation i.e. extensions of the URI “family” for ENUM.

The really challenging combinations are when an originator (A-number, with its current and potential applications) is faced with the B-number associated list, where traditional Basic Calls are non-existent or not preferred. Then there has to be some kind of intelligent choice between the alternatives and in some instances there may be more than one application/terminal used simultaneously (i.e. sending an e-mail to an e-mail and SMS simultaneously).

12. ENUM TRIAL PLANNING

The following points are deemed to fall outside of the original TCF ENUM Working Party Scope of Work. The following sections – ENUM Trial Planning, Scenarios for a New Zealand Trial, Where To Next, and a High Level Work Plan outline much of what is required to initiate an ENUM trial. This section is in no way exhaustive but canvasses input from both the ENUM Working Party and overseas trial and experience.

12.1 Stage 1 Objectives Prior to a Trial

The Parties agree that the high level objectives prior to any ENUM trial are as follows:

a. Identify the business model(s) and high level costs of creating an ENUM mechanism within the New Zealand environment;

b. Define the commercial model(s) of the Tier 1 Registry and ENUM Registrar functions that will operate during the trial and ideally for commercial ENUM use;

c. Define the policies, principles and codes of practice involved in implementation and use of ENUM-enabled services (as above) for both trial and potential commercial implementation;

d. Determine the legal requirements for trial and commercial implementation including enforcement;

e. Determine the end-user requirements for trial and commercial implementation with particular emphasis on privacy, authentication, validation, potential uses and customer models;

f. Identify issues and risks for resolution / research;

g. Clarify regulatory and other requirements including the impact on current codes and number administration;

h. Participate in international standards bodies and ENUM working parties; and

i. Prepare a recommendation to the TCF Board on ENUM and Stage 2.

12.2 Stage 2 Objectives of an ENUM Trial

The Parties agree that the high level objectives of the ENUM trial are as follows:

a. Define and agree architectures (network, service, interconnect, billing, registry / registrar and validation) for implementation of ENUM capabilities;

b. To evaluate the pros and cons of the defined architecture for implementation of ENUM capabilities, with particular emphasis on demonstration of the Registry and Registrar functions;

c. To evaluate the processes, interfaces, and protocols for the interactions between seven functional categories involved in implementation and use of ENUM-enabled services, which include Tier 1 Registry, ENUM Registrar, ENUM Tier 2 name service provider, telecommunication service

provider, application service provider, authentication agency (AA), and ENUM Users (the "Functional Categories");

d. To determine technical and operational requirements to provisioning ENUM records at Tier 1 and Tier 2 levels;

e. Agree and apply for e164.arpa delegation for the trial period;

f. To assess DNS requirements and implications in the provision of ENUM-enabled services;

g. To determine security and verification requirements for provisioning and operation of ENUM-enabled services;

h. To determine privacy requirements and implications in the provision of ENUM-enabled services;

i. To test from technical and user perspectives applications that employ or rely on the use of ENUM capabilities;

j. To allow Participants and interested parties to assess the economic benefits and costs of supporting ENUM services; and

k. To prepare a report of the trial for distribution to all relevant authorities and to the public.

12.3 Responsibilities of Parties

The Parties accept the respective responsibilities outlined below. The Parties agree to fulfill their respective responsibilities in conducting the trial.

a. The TCF will direct and monitor the trial;

b. The TCF will contract with a project manager (Project Manager) who will assist the TCF in overseeing the conduct of the trial. The TCF will bear the costs of the contract with the Project Manager;

c. Participants who are eligible to receive allocations under the NAD will apply for the assignment of numbers for use in the trial, and will manage any numbering resources assigned;

d. The TCF will determine the length of the trial. The trial shall comprise three phases: Phase 1 - Registry Infrastructure; Phase 2 - Registry/Registrar Interface; Phase 3 -Application Testing. The combined length of these three phases shall not exceed the length of the temporary delegation of numbering resources necessary for the conduct of the trial;

e. The TCF, with assistance and input from Participants, will develop a trial plan (Trial Plan) that outlines the procedures to be followed in conducting each phase the trial. The Trial Plan will identify the data and documentation to be generated in conjunction with or as a result of the testing procedures (Trial Materials). It is anticipated that the Trial Materials will include all documents, data, technical specifications and models, and other specifications and models, and other contributions or outputs generated during the trial. Trial Materials will not include Participants' confidential and/or proprietary business information, personal data provided by users and entered into the DNS and/or registry/registrar systems or other proprietary information used or generated during the trial;

f. Participants will comply with the Trial Plan, and will make all Trial Materials available to one another and to the TCF for the purpose of

drafting and finalizing a report of the trial. Participants may also engage in other testing activities, provided that such activities do not in any way disrupt the Trial Plan or alter the results of the Trial Plan. Participants will not be required to account to one another or to the TCF for the results of such additional testing activities;

g. Participants will comply with the NAD but will seek to incorporate terms agreed by the TCF for the use of numbering resources allocated under the NAD for the trial[4];

h. Where feasible, the Parties will make decisions regarding the trial by consensus. When, in the judgment of the Project Manager, consensus regarding one or more decisions cannot be reached in a timely fashion, the Project Manager will refer the decision(s) to the TCF Board for final resolution;

i. The Parties will act in a transparent, non-arbitrary and reasonable manner in the conduct of the trial;

j. Each Participant will designate one primary and up to two alternate individual representatives who will sit on a TCF Participants' Working Group and will serve as the point of contact between the Participant, and TCF, the Project Manager, and all other Participants in the trial. The TCF Participants' Working Group will meet fortnightly by conference call. Communications or notice of any kind directed to the Participant's representative will be considered to have been directed to the Participant. In the event that the Participant's representative is unavailable, the Participant will be solely responsible for arranging for an alternate representative to attend TCF Participants' Working Group meetings and to receive communications from the TCF, the Project Manager, and other Participants;

k. Participants will each bear all of their own costs and expenses of participating in the trial. Neither compensation nor financial benefits are foreseen for any Participant in the conduct of the trial;

l. Participants will cooperate with the Project Manager, with the TCF, and with one another in the conduct of the trial and in the drafting of the report of the trial;

m. Participants commit to remain actively involved for the full duration of the trial and the time required to draft a report of the trial, subject to the approval of the TCF, and will use reasonable best efforts to ensure the success of the trial. Participants agree that sustained active involvement by each Participant, which includes but is not limited to regular attendance at meetings of Participants and contribution to reporting the results of the trial, are prerequisites to such success;

n. Participants' trial activities must be limited in scope to one or more of the Functional Categories involved in implementation and use of ENUM-enabled services. Participants will identify the Functional Category(s) in which they will operate for the duration of the trial at the time of executing the legal agreement setting up the trial;

o. The Parties will endeavor to recruit a sufficient number of Participants in each of the Functional Categories to ensure the success of the trial. The

[4] There may also be constraints in the NAD and the Rules that need to be considered and worked through for the ENUM trial.

TCF may permit additional Participants to join the trial after the trial commences if, in the sole discretion of the TCF, adding a new Participant to the particular Functional Category(s) in which the prospective participant is interested will be reasonably feasible and useful to the trial as a whole. No prospective participant will be permitted to join the trial at any time unless that prospective participant first executes the appropriate legal document;

p. Participants will use reasonable best efforts to ensure the continuity of the trial. In the event that any Participant is prevented or prohibited from completing the trial for any reason, that Participant will, at the direction of the TCF, transfer all Trial Materials in that Participant's possession to another Participant or Participants to be designated by the TCF;

q. At the completion of the trial, Participants, under the direction of the Project Manager, will produce a draft report for the approval of the TCF. Each Participant will contribute to the drafting of the report, and each Participant will be required to contribute Trial Materials to the report pursuant to the Trial Plan; and

r. The TCF will finalize the report of the trial and will ensure that it is distributed to relevant authorities and to the public. The final report will contain an express waiver of any representations or warranties regarding the accuracy, completeness, or fitness for particular purposes of the contents.

12.4 Scenarios for a New Zealand Trial

The Working Party acknowledges a combination of applications can be selected for a future trial – but the trial outcomes must have tangible results and test the core potentials of ENUM - without the requirement of far-fetched service development, but still providing services of value to end-users:

a. A set of 'Basic Calls':

   - SIP to SIP (IP telephone to IP telephone)

   - PSTN (Fixed telephone) to SIP (IP telephone) and reverse;

b. MOBILE (3G endpoint) to SIP (IP telephone) and reverse;

c. Information service;

d. E-mail to e-mail via E.164 number;

e. Http to http;

f. Maintenance service – End user can add, modify, delete data in DNS; and

g. At some stage seek cooperation with ENUM activity in another country (preferably Australia) to test international calls corresponding to the suggested 'Basic Calls' as illustrated above.

At least at first glance it seems to be more difficult to utilise ENUM when a session is originated from PSTN/ISDN or MOBILE networks to SIP than from SIP to these networks. This is due to the more open and flexible (but less controlled) environment of the Internet architecture. When routing calls from PSTN/ISDN/MOBILE there needs to be a gateway in some sense. However the more controlled environment of traditional telecom networks may prove to be more secure, reliable, performance and of better accountability and quality than Internet – at least for some services.

Requirements of performance should be specified and measured: Examples may be: volumes, hits, hits/volume ratio, record size, update frequency, type of URI (tel, sip, email, http).

12.5 High Level Work Plan

The ENUM Trial should be undertaken with the objective of establishing the feasibility of a permanent implementation. It is therefore imperative that a clear point in time for ending the trial has to be set. After the trial, the TCF should sum up the conclusions reached and report to the MED. Otherwise any external ENUM trials might be a starting point for illegal functions that are not based on regulation and legislation, and thus lack the foundation necessary to be satisfactory for involved parties either governmental or commercial in nature. A cost model for the Tier-1 hierarchy should also be studied with regard to what customer relationships will evolve, and which participants have a contractual agreement with entities that fall outside traditional interconnect relationships.

Outlining the specific implementation procedures, potential revenue flows, regulatory requirements, and administrative policy or process demands during a trial are vital. Previous User ENUM trials offshore have focused singularly on technical issues, but equally important are the administrative processes and the economical flow between participating parties.

Prior to an ENUM trial being undertaken in New Zealand, there are serious questions that have not been investigated far enough by the TCF, let alone the wider industry:

- Is there existing demand for User ENUM services in New Zealand?
- Is there existing demand for Operator ENUM services in New Zealand?
- Which Tier-1, Tier-2 and Tier-3 entities are participating in an ENUM trial?
- Are the participants (User or Operator) in the trial supportive of ENUM?
- Will the ENUM trial interact with Ex-Directory database information?
- Will the ENUM trial interact with the number portability database records?

To ensure both the national number plan is protected, appropriate security mechanisms for subscriber privacy within ENUM must exist and participants will require large investment at the Tier-1 and Tier-2 levels. Is this acceptable to trial participants?

The TCF ENUM Working Party has subsequently designed a working plan based on experiences from trial offshore that aims at exploring the market interest in ENUM and prerequisites and consequences of a pilot.

Based on the activities of the Swedish Government's Postal and Telecommunications department, the work can be organised in three working groups as follows:

12.6 INF_ENUM – Infrastructure and ITU delegation.

The purpose is to study the requirements for creating a common infrastructure to enable Operator (or Infrastructure) ENUM at the country code level (Tier 1- role) during a trial, so that suitable develop guidelines regarding the delegation of the domain .4.6.e164.arpa are created.

12.7 DOM_ENUM – ENUM domain names and customer process.

The purpose is to study the registration and customer process regarding ENUM subscribers, remuneration principles between participants, and evaluate who can act within a semi-trusted (yet secured) ENUM Registrar and nameserver hierarchy.

12.8 APP_ENUM – Applications

The purpose is to investigate which applications based on ENUM should be part of the trial.

Drawn from the Swedish Trial, below are eleven tasks that were assigned to the INF_ENUM working group in the initial PTS work plan. The working group has not found reason to deviate from this planning, although many of the topics have to a larger depth been penetrated by other groups both under an ETSI and IETF umbrella.

No	Name	Description
1	**Application inventory**	To study which applications based on ENUM, according to RFC 2916, may be suitable for the NZ market.
2	**Application selection**	Select a suitable set of applications that should be included in the pilot.
3	**Customer type description**	Describe the customer type for the applications tested in the pilot.
4	**End user criterias**	Specify what criteria should be used in selecting the end users participating in the pilot.
5	**Type of E.164 numbers**	Specify which type of E.164 number in the NZ number plan that should be included in the pilot.
6	**Identify organisations**	Identify the different organisations (from a functional perspective) that will be involved in delivering the applications in the pilot. Document these different architectures, on the Tier 1 as well as the Tier 2 level, and in addition describe what role the application vendor will have in relation to the other organisations.
7	**Competition**	Identify at what levels, concerning ENUM, competition can occur.
8	**Registration reqs**	Specify the requirements by the application chosen for the pilot, will have on the registration- and customer processes.
9	**Personal data reqs**	Specify the requirements, applications chosen for the pilot, on the management of the end-customer personal data.
10	**National infra-structure reqs**	Specify the requirements the applications chosen for the pilot will have on the common infrastructure for ENUM in New Zealand.
11	**Global Infra-structure reqs**	Specify the requirements that the applications chosen for the pilot will have on the global infrastructure for ENUM.

13. NEXT STEPS

The advent of a global Infrastructure seems to be a natural progression as a result of the current work being undertaken by the various standards bodies. If such shift were to happen, the following steps are likely to occur. These are not sequential, and can be implemented at any time as a standalone system.

13.1 Current (Traditional) Situation on the PSTN

CSPs on the PSTN using TDM technology switch calls via traditional TDM PoI's using conventional call routing methods.

Note: PSTN is specified, but also includes ISDN and PLMN.

13.2 Step 1: CSP Islands connected via PSTN

- CSPs migrate from TDM to IP technology within their own networks.
- Connectivity to other CSPs is via IP/TDM gateways using conventional signaling (SS7). At the PoI, each CSP still appears to be using TDM technology.
- Calls originating or terminating in the CSPs IP network are routed to the PSTN or are incoming from the PSTN.
- The signaling and media in the IP network has no connectivity to any other IP networks or the Internet. (Intranet approach).

This is happening now in the New Zealand market and requires no additional public infrastructure.

13.3 Step 2: Private Infrastructure ENUM only

- CSPs will use infrastructure ENUM for routing within their own networks.
- The CSP will set up its own DNS infrastructure. This will include its own domain apex (Tier 0), Tier 1 and Tier 2. CSP provides its own internal Registry function.
- The NAPTR records in the DNS contain either internal user end-point information or routes to the PSTN.
- Connectivity with other CSPs is still via traditional means as in Step 1.
- No single common external apex required
- Infrastructure ENUM may or may not indicate routing to other networks (CSPs).

13.4 Step 3: Private Infrastructure with IP based Interconnect

- CSPs interconnect their IP networks with other IP based networks on a bi-lateral basis.
- Connectivity with other CSPs without IP PoIs via the PSTN, as in Steps 1 & 2.

- The NAPTR records in the DNS contain either internal user end-point information, IP based routing or routes to the PSTN.
- No single common external apex required.
- Infrastructure ENUM may or may not indicate routing to other networks (CSPs).

13.5 Step 4: CSP-shared Infrastructure ENUM with Extranet between a Group of Service Providers

- Participating CSPs require connectivity via a shared extranet.
- Each CSP owns internal network (Intranet), the existing PSTN connections and any IP based interconnects are also connected to the extranet via additional border elements.
- A CSP-shared Infrastructure ENUM is set up on the extranet.
- Required elements are:
  - a CSP-shared domain apex within the extranet;
  - shared Tier 0/1 and hence a CSP-shared external Registry;
  - The NS records in the common Tier 1 point to the Tier 2 nameserver of the participating CSPs;
  - The CSP's Tier 2 Nameserver is connected to the extranet and only holds NAPTR records for the specific number ranges hosted by the CSP;
  - The same DNS infrastructure as in Step 2 & 3 is required by the CSP. The major difference being that it only requires to keep entries which belong to numbers hosted by themselves. All other entries can either be deleted or replaced with default entries which point to the border elements from inside the CSP's network; and
  - The CSP's internal DNS is overlaid to the shared (extranet) DNS. This means that if a CSP queries a number they host themselves, the answer comes from its own DNS; if it is querying a number hosted by another CSP, its internal DNS passes the query to the extranet and the answer comes from the Tier 2 nameserver of the CSP hosting that number.

Each participating CSP's internal (intranet) DNS is still fully under its own control. The Tier 0/1 Registry is under CSP-shared control, and the Tier 2 nameserver in the extranet is under the control of the CSPs.

This step, the provisioning of a CSP-shared Tier 0/1 and prior agreement by the participating CSPs on how this is set up, is mandatory.

13.6 Step 5a: Common Infrastructure ENUM within a Global Shared Extranet

If several independent groups of CSPs all implement Step 4 above, the possibility of creating a common shared extranet now exists. This can be achieved in two ways:

a. The groups retain their CSP-shared extranets and a new common shared extranet is overlaid on top. This method is in principle the same as repeating Step 4 with each participating CSP now being replaced by groups of CSPs. This method is not recommended.
b. The groups merge their CSP-shared extranets. This approach is more

simplistic, but may cause issues with potential duplicates of IP addresses, registries and/or namespaces.

As a result of the potential duplication issues arising out of (the preferred) method B, it is strongly recommended to plan for a common shared extranet from the beginning.

13.7 Step 5b: Public Infrastructure ENUM on the Internet.

- A group of CSPs may elect to use the public Internet as a CSP-shared network from the beginning; or
- Two extranets may be merged using the Internet as a common shared Infrastructure ENUM.

Any domain can be used as the Tier 0/1 apex. This gives the possibility of more than one public Infrastructure ENUM system.

14. CONCLUSIONS

For the most part these are based around the Scope of Work the ENUM Working Party has been requested to address. In our investigative process, there have been some conclusions drawn that fall outside of the initial scope, but are deemed important and so therefore are included.

14.1 Summary of Trials:

- Every User ENUM trial to date has been successful in proving one thing - the public DNS infrastructure works.
- The WP does not consider that a trial which only proves DNS capabilities to be of any significant value, and therefore would not endorse any trial which does not attempt to address the security, policy and governance issues.
- The common outcome of these trials is that there is a lot more work required in the areas of policy/governance, security, authentication/validation etc. As a result of this, there has been substantial work carried out by the individual standards bodies in an effort to address these concerns. A number of these pieces of work are due to be ratified in the coming months.
- Previous trials (particularly the UK and Austria) have identified a need for User ENUM to co-exist with an Infrastructure ENUM environment. This has arisen from a realization that the issues around security and privacy are difficult to address. The "trusted" controlled nature of Private Infrastructure ENUM goes a long way to mitigating these concerns.
- Overseas regulators are interested in ENUM, and to a greater or lesser extent, participate in the trials. No regulation of ENUM has yet been considered.
- Any future ENUM trial in New Zealand, whether User or Infrastructure, must not limit the ability for NZ to participate in any future globally defined Infrastructure ENUM implementation. Current draft standards by ETSI are addressing the issues around global Infrastructure ENUM implementation. These drafts are due for ratification in the near future.
- The Internet New Zealand User ENUM trial basically proves DNS infrastructure – which already works and has already been proven in past overseas ENUM trials. The InternetNZ trial misses key aspects including validation, numbering, carrier issues and privacy concerns. Additionally, overseas disjoints and issues are unaddressed. Further, it may result in a registry model (Tier 1) that doesn't fit New Zealand's long term requirements. However, Internet NZ's work on the PUA is positive, as is ETSI liaison.

Recommendations:

- ***Any TCF sanctioned trial should encompass Infrastructure and User ENUM, and firstly determine policy, principles, codes of practice, legal requirements, customer requirements and an appropriate model - including architecture, registry / registrar and domain trees - for eventual use prior to the actual trial.***
- ***The TCF Board should not support or endorse the proposed InternetNZ User ENUM Trial in its current form.***

14.2 Potential Effects of ENUM on Current and Draft Codes

- To avoid increased risk, additional issues and probable delays to the introduction of number portability, any ENUM trial should be deferred until after the successful implementation of number portability in New Zealand. Ideally there would be ongoing use of the resource, knowledgebase and design aspects to overlay ENUM on to number portability.
- No significant effect on other TCF Codes have been determined at this time

Recommendation:

- ***Any TCF involvement in an ENUM trial should be deferred until after the successful implementation of number portability in New Zealand. This is to ensure that the LMNP project is not impeded in any way by an ENUM work-stream.***

14.3 Transition and Interoperability Issues

- Existing interconnect relationships between telecom network operators should form the basis of planning for an Infrastructure ENUM trial, bringing in ETSI work. The TCF should be the coordination point for this.

Recommendation:

- ***Further investigation is needed for interoperability and transition. Such work is separate to this working party.***

14.4 Numbering

- If an ENUM trial is to proceed in New Zealand, be it with or without TCF involvement, it should only proceed after dialogue with the NAD with respect to agreeing the number blocks (and correct use of those blocks) used for that trial. A common mistake identified from previous trials is not separating out a range solely for trial use. This approach will alleviate any negative effects that an unsuccessful trial may have on users of the PSTN. In addition to this, ranges have also been broken out for use with VoIP services.
- The abuse or compromising of the E.164 number plan during a User ENUM trial could potentially be seen by the public as negligence on the part of the telecommunications operators providing PSTN or mobile services, and not the Tier 2 Registrar ENUM service provider.
- In order to mitigate the above point, any trial, even if User ENUM only, must use a separate non-geographic number range endorsed by the members of the NAD.
- The UK findings show that using geographic numbers as ENUMs caused significant problems, especially with number portability. In the UK, PSTN (locally known as PATS) numbers are in the same geographic range as VoIP services. PSTN services are subject to portability, but VoIP services are not. This caused confusion for both service providers and PSTN users alike.

Recommendation:

- ***No numbers be allocated until the scope of a trial has been agreed by the TCF and the policy, principles, and codes have been drafted.***

14.5 Assignment of the New Zealand ENUM Delegation (.4.6.e164.arpa)

- The relevant standards bodies from both the Internet and telecommunications communities are signaling a desire for some 'commonality' between ENUM implementations globally. This was endorsed by Tony Holmes (Chair of the ETSI ENUM Workshop Steering Group) at the workshop in Auckland (24/03/2006).
- If Infrastructure ENUM is to go ahead, careful planning is required. ETSI recommend that the e164.arpa domain be used for infrastructure ENUM also. The infrastructure tree should be below the ccTLD e.g.: 4.6.e164i.arpa. This structure below this would then be a matter for the CSPs involved in the Infrastructure ENUM.

Recommendation:

- ***The .4.6.e164.arpa delegation should be held by the MED and not be assigned for trial purposes until a meaningful trial, as outlined in this report begins, or InternetNZ and the TCF Board jointly agree differently.***

14.6 ENUM Registry Structure and Policy Framework

- A common industry body must be formed that will set the policy, codes of practice, arbitrate disputes and enforce appropriate sanctions for all participants in the supply of ENUM enabled services.
- An accreditation process is necessary.
- Some jurisdictions have found it necessary to bind ENUM into their legal framework to ensure accountability of parties participating in the delivery of ENUM.
- Authentication, (Validation + Identification), are commonly viewed as an important element for ENUM success.
- An effective authentication process will directly relate to consumer confidence in ENUM. This point has been endorsed by the Austrian trial where they noted that due to privacy concerns User ENUM was essentially relegated to a VoIP only service.
- There is some value to be gained from monitoring the development of the UK CRUE (Carrier Registration in User ENUM) initiative. The CRUE model has been devised as a measure to ensure a more rigorous process for validation in User ENUM.
- From a carrier's perspective, before ENUM is viable in NZ, work needs to be done defining and establishing robust VoIP peering arrangements to ensure interconnect transactions can occur with a comfort level around billing accuracy and non-repudiation.
- Overseas countries have invested heavily both in terms of manpower and policy formulation to facilitate their respective Public User ENUM or Private Infrastructure ENUM trials. As a result, acknowledgement of the wider investment required by both Governmental and industry entities is required.

Recommendation:

- **The TCF Board needs to decide whether to allocate such resource, so as to facilitate the necessary planning for a New Zealand ENUM deployment, as set out in Stage 1 of ENUM Trial Planning; or facilitate support of the future Internet NZ ENUM activities with appropriate planning and assistance.**

15. REFERENCES

ACA (2002) 'ENUM' Australian Communications Authority, at http://www.acma.gov.au/ACMAINTER.65646:STANDARD:2106794102:pc=PC_2475

ACA (2002b) 'Introduction of ENUM in Australia - Discussion Paper', Australian Communications Authority, September 2002, at http://www.acma.gov.au/ACMAINTER.65646:STANDARD:2106794102:pc=PC_2319

APF (2002) 'Submission to the Australian Communications Authority re ENUM', Australian Privacy Foundation, 2 November 2002, at http://www.privacy.org.au/Papers/SubmnACA021102.html

Borland J. (2001) 'Technology uses one number to find you on any device' Nowhere to hide column, CNet News, 17 May 2001, at http://news.com.com/2102-1033-257704.html?legacy=cnet

Clarke R. (1999a) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' Proc. User Identification & Privacy Protection Conf., Stockholm, 14-15 June 1999, at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

Clarke R. (1999b) 'Person-Location and Person-Tracking: Technologies: Risks and Policy Implications' Proc. 21st Int'l Conf. Privacy and Personal Data Protection, 13-15 September 1999, pp.131-150. Revised version in Information Technology & People 14, 2 (Summer 2001) 206-231, at http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html

Clarke R. (2001) 'Persons at Risk', in 'Research Challenges in Emergent e-Health Technologies', July 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html

Cybertelecom (2002) 'DNS: ENUM', at http://www.cybertelecom.org/dns/enum.htm

Darling P. (2002) 'NGN Issues - Numbering and Addressing', Australian Communications Industry Forum, at http://www.acif.org.au/ngn_fog/files/FOG03_001.pdf

DTI-UK (2004) “ENUM – Consultation on Proposed Arrangements”, at http://www.dti.gov.uk/consultations/files/publication-1286.pdf

ENUMLLC, “Memorandum of Understanding for an ENUM trial in the United States”, at http://www.enumllc.com

EPIC (2001) 'ENUM', at http://www.epic.org/privacy/enum/default.html

ETSI Draft ETSI TR 102 055 (2005-01) – Infrastructure ENUM, at http://www.etsi.org

ETSI TS 102 051v1.1.1(2002-07) – ENUM Administration in Europe, at http://www.etsi.org

Haberler, M. (2005) “Combined User and Carrier ENUM in the e164.arpa tree” (draft), IPA & OEFEG.

Holmes, T. (2006), “New Zealand workshop presentation & personal slides”, British Telecom & ETSI ENUM Working Group Chair.

Huston G. (2002) 'The Lord of the Numbers', ISP Column, May 2002, at http://www.potaroo.net/ispcolumn/2002-06-enum.html

IETF (1997) 'Dynamic Host Configuration Protocol, RFC 2131, March 1997, at http://www.ietf.org/rfc/rfc2131.txt

IETF (1999) 'SIP: Session Initiation Protocol', RFC 2543, March 1999, at http://www.ietf.org/rfc/rfc2543.txt

IETF (2000a) 'A DNS RR for specifying the location of services (DNS SRV)', RFC 2782, February 2000, at http://www.ietf.org/rfc/rfc2782.txt

IETF (2000b) 'URLs for Telephone Calls' RFC 2806, April 2000, at http://www.ietf.org/rfc/rfc2806.txt

IETF (2000c) 'The Naming Authority Pointer (NAPTR) DNS Resource Record', RFC 2915, September 2000, at http://www.ietf.org/rfc/rfc2915.txt

IETF (2000d) 'E.164 number and DNS' RFC 2916, Internet Engineering Task Force, September 2000, at http://www.ietf.org/rfc/rfc2916.txt

IETF WG (1998-) '', at http://www.ietf.org/html.charters/enum-charter.html

InternetNZ/M-Co (2005), “The staging of the first ENUM trial in New Zealand”, at http://www.internetnz.net.nz/pdfs/proceedings/tf/enum/2005-07-ENUM-Trial-Report-complete.pdf

ITAC-T (2001) 'Report of the Department of State ITAC-T Advisory Committee Study Group A Ad Hoc on ENUM', 6 July 2001, at http://www.nominum.com/ENUM/2001-07-06-ENUM-Report-Department-of-State-Final.doc (viewed and printed in late 2001, directory no longer accessible on 18 November 2002)

ITU (2001) 'ENum' International Telecommunication Union, at www.itu.int/osg/spu/enum/index.html

ITU (2001) 'ITU ENUM Activities' International Telecommunication Union, at http://www.itu.int/infocom/enum/index.html

Lessig L. (1999) 'Code and Other Laws of Cyberspace' Basic Books

Lind, S. (2005) “Infrastructure ENUM Requirements Draft”, AT&T

NGI (2001-) 'ENUM Reference Materials', Center for Next Generation Internet, at http://www.ngi.org/enum/

NLEG (2002) “ENUM in the Netherlands”, A report by the Dutch ENUM Group, at http://www.enuminnederland.nl

Pfautz, P. (2001) “ENUM administration major issues”, AT&T, at www.itu.int/osg/spu/**enum**/workshopusafeb12-13/pfautz.ppt

RIPE (2002) 'RIPE Database Reference Manual', 15 August 2002, at http://www.ripe.net/ripe/docs/databaseref-manual.html

Rosencrance L. (2001) 'Phone number-to-e-mail service raises privacy concerns' Computerworld, 5 October 2001, at http://www.computerworld.com/printthis/2001/0,4814,64475,00.html

Rutkowski A. (2001) 'The ENUM Golden Tree: The Quest for a Universal Communications Identifier' inform 3, 2, April 2001 (97-100), at http://www.ngi.org/enum/pub/info_rutkowski.pdf

Schafer, R. (2003) "ENUM in the US – RIPE 46", MCI network Architecture & Standards

Shockey R. (2002) 'Privacy and Security Considerations in ENUM', Internet Draft, October 2002, at http://www.ietf.org/internet-drafts/draft-shockey-enum-privacy-security-00.txt

Stastny, R. (2005) "Analysing the lessons learned from ENUM implementations in Austria", OFEG, at http://www.oefeg.at

Stastny, R. (2005) "ENUM Tutorial Part 1 -5", Miami Summit 2005, at http://voipandenum.blogspot.com/

The Times (2001) 'One number & and no escape anywhere' The [London] Times, 3 September 2001, at http://www.thetimes.co.uk/article/0,,3-2001303964,00.html

UKETG (2004), "Status Report on the trial implementation of ENUM in the UK"

US Department of State (2005), "Terms & Conditions for a US Trial of ENUM".

APPENDICES:

APPENDIX A: Draft ETSI TR 102 055 (2005-01) - Infrastructure ENUM

Likely Infrastructure ENUM usage scenarios

IMS-based NGN providers may either control/manage their own communications network, being also a communication network provider, or provide their service as an application on the Internet.

The subscribers may have access to the above mentioned end-points either via the Internet, via dedicated networks or even via the PSTN.

The primary questions are, depending on the peering architecture chosen by IMS-based NGN providers:

- How do I find the ingress PoI (or IMS servers) of a IMS-based NGN provider hosting a certain E.164 number, if a common network infrastructure is used?
- How do I find the egress PoI from within the own network if no common infrastructure is used?
- What are the options available for the Infrastructure ENUM architecture for the above mentioned cases?
- What are the Identifiers used to address the ingress or egress PoIs within ENUM? (URIs used within NAPTR).

Some examples are shown below of the likely infrastructure ENUM usage scenarios as introduced in Section 9.

Private Infrastructure ENUM only (Step 2)

A CSP is using Private Infrastructure ENUM only within its own network (Intranet). There are only connections to the PSTN via IP-Gateways.

Infrastructure ENUM is used to find end-users in their own network (Intranet) and the proper gateway for calls routed to the PSTN.

All E.164 numbers not assigned to end-users are routed to the PSTN gateways.

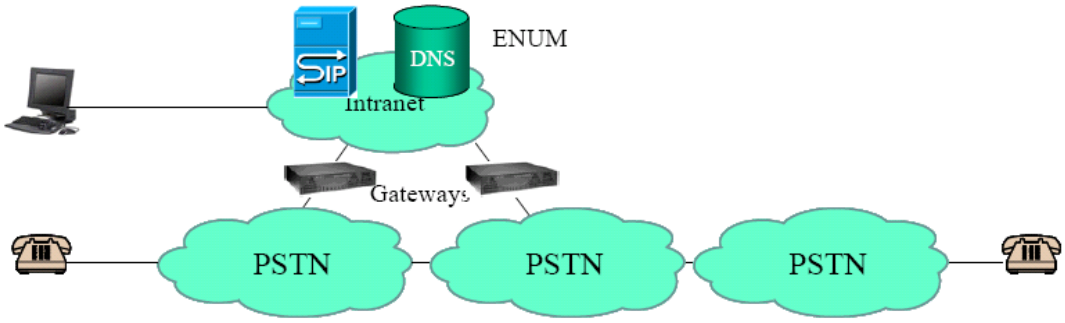
The Infrastructure ENUM database may be implemented in any DNS domain at the CSP discretion and holds the following information:

For every end-user within the CSPs network a zone entry in ENUM exists for the related E.164 number.

For numbers ported out to other operators also a zone entry exists for the related E.164 number. It contains an “sip” or “h323” URI pointing to the gateway serving either directly the ported out number or a transit network. The zone entry may also contain a “tel” URI with a routing number. The NAPTR RR containing the “tel” URI will then be used by the gateway. If only one gateway exists to the PSTN, the zone entry may only contain the “tel” URI and the routing to the gateway may be done by default.

Numbers out of the number range assigned to this network but not assigned to end-users (unassigned numbers) must contain a NAPTR with enumservice “void” as all numbers will be entered in the DNS. This could be handled with a common NAPTR at the zone related to the whole number range as described in TS 102 172.

Number ranges not assigned within this network may contain a “wild card” NAPTR at the zone related to the number range pointing to a PSTN gateway serving this number range. Number ranges not assigned to any operator should contain a NAPTR RR with enumservice “void”.



Private Infrastructure ENUM with IP-based Interconnect

A CSP is using Private Infrastructure ENUM only within its own network (Intranet), there are connections to the PSTN via IP-Gateways and in addition there are direct IP-based connections to other CSP via border elements.

Infrastructure ENUM is used to find end-users in their own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

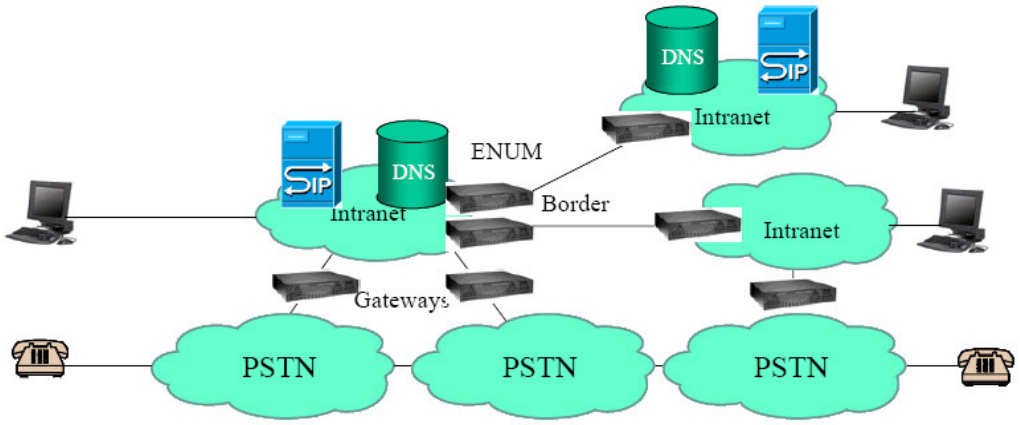
Numbers out of the number range assigned to this network but not assigned to end-users (unassigned numbers) must contain a NAPTR RR with enumservice “void” as all numbers will be entered in the DNS. This could be handled with a common NAPTR RR at the zone related to the whole number range as described in TS 102 172.

Number ranges not assigned within this network should be routed either to SCN Gateways or to the border elements.

In this step, the Infrastructure ENUM database may be implemented in any DNS domain at the CSP’s discretion and holds in addition to the information described in the above section also NAPTR RRs pointing to the border elements.

These NAPTR RR contain “sip” or” h323” URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. sip:+4319793321@border1.prov.net

The border elements in the other CSPs are querying their own private Infrastructure ENUM database to route the call further in their own Intranets.



Shared Infrastructure ENUM with Extranet

A CSP is using Private Infrastructure ENUM within his own network (Intranet), there are connections to the PSTN via IP-Gateways and in addition there are IP-based connections to other CSP via border elements and via an extranet.

Private Infrastructure ENUM is used to find end-users in their own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

The routing in the extranet is done via the Shared (or Common) Infrastructure ENUM database in the extranet.

For the routing of calls to and within the extranet two options exist:

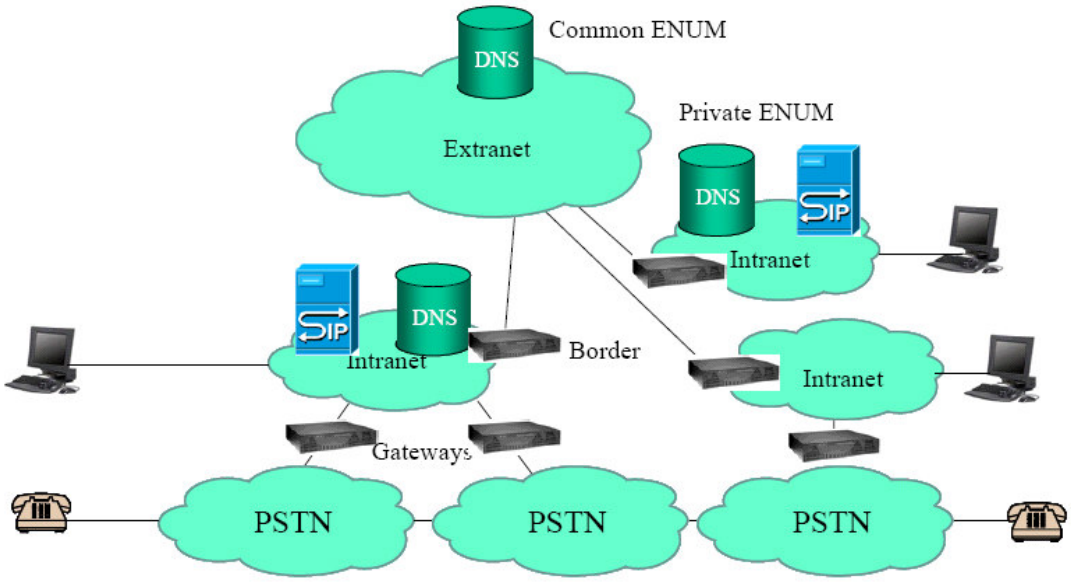
1. The extranet and the Intranet are completely separate. In this case the calls are routed in the Intranet to the Border Element and the Common Infrastructure ENUM database in the extranet is queried by the Border Element to find the proper routing information within the extranet. The Private ENUM Infrastructure database and the Shared ENUM Infrastructure databases may be in different domain trees, and only the border elements need access to the shared database. In this case three Infrastructure ENUM queries may be necessary to complete a call between CSP A and CSP B. First CSP A need to query his private Infrastructure ENUM database to find the Border Element to the CSP shared extranet. The Border Element from CSP A needs to query the CSP-shared Infrastructure ENUM database to find the address of the ingress Border Element of CSP B, and the Border Element of CSP B needs to query the private Infrastructure ENUM database of CSP B to finally find the AoR of the end-user.

2. The Private and the Shared Infrastructure DNS are using the same domain tree and the data in the CSP-shared Infrastructure ENUM are visible from within the Intranet (Split DNS). In this case the Border Element of the other CSP may be addressed directly, thus saving the second query and also saving the separate administration of the different trees.

All E.164 numbers not assigned to end-users are routed either to PSTN gateways or to the border elements. In this scenario, unassigned numbers may, at the sole discretion of the CSP responsible for these numbers, be indicated in the shared database. If these are so indicated, the querying CSP can choose to process the call failure, without passing it onwards.

The Private ENUM database may be implemented in any DNS domain at the CSP discretion and holds in addition to the information described in the above section also NAPTR RR pointing to the border elements (option1) or is derived directly from the Public Infrastructure ENUM (in option 2)

These NAPTR RRs contain “sip” or “h323” URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. +4319793321@border1.prov.net.



Shared Infrastructure ENUM on the Internet
A CSP is using Private Infrastructure ENUM within its own network (Intranet), there are connections to the PSTN via IP-Gateways and IP-based connections to other CSP via border elements and the public Internet. In addition there may also be connections via border elements and an extranet or dedicated connections.

Private Infrastructure ENUM is used to find end-users in their own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

The routing on the Public Internet is done via the Shared Infrastructure ENUM database in the Public Internet.

The CSP may also be part of the public Internet, so that their end-users and the SIP-Servers are reachable on the public Internet.

For the routing of calls to and within the public Internet the following options exist:

a. The public Internet and the Intranet are completely separate. In this case the calls are routed in the Intranet to the Border Element and the shared Infrastructure ENUM database on the Internet is queried by the Border Element to find the proper routing information within the Internet. The Private ENUM Infrastructure database and the shared ENUM Infrastructure Databases may be in different domain trees. As described in the section above, up to three Infrastructure ENUM queries may be necessary to complete a call;

b. The Private and the shared Infrastructure DNS are using the same domain tree

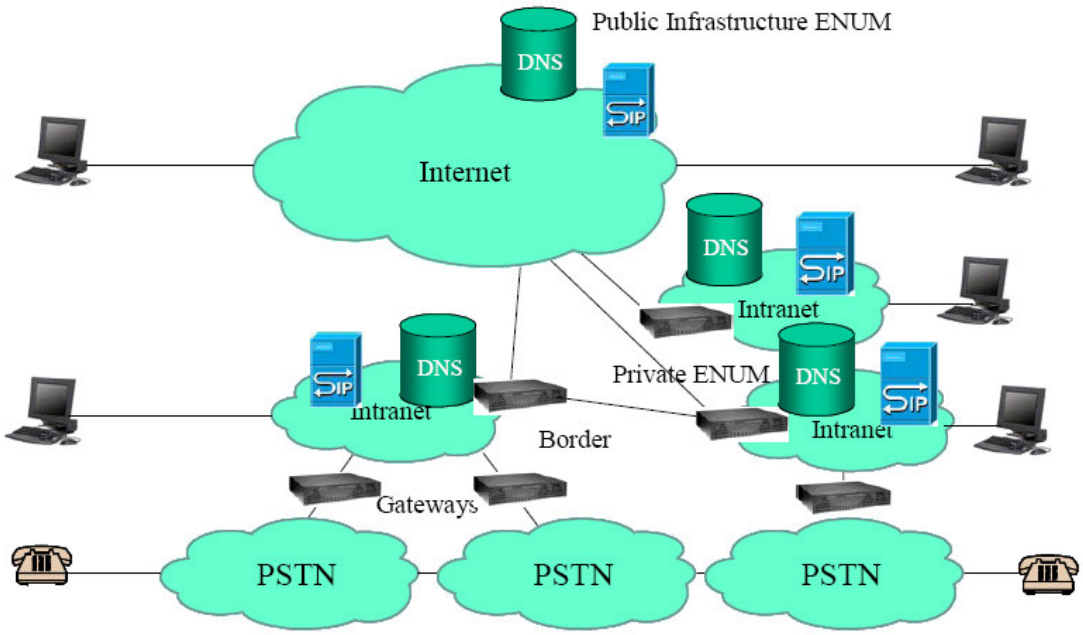
and the data in the shared ENUM Infrastructure are visible from within the Intranet (Split DNS). In this case the Border Element of the other CSP may be addressed directly, thus saving the second query and also saving the administration of the routing to other CSPs; and

c. Since CSPs may also have their end-users on the public Internet and do not want to hide these users behind a border element, CSP may populate the Public Infrastructure ENUM database also with end-user data. In this case it is recommended that this data is not visible to other end-users directly.

All E.164 numbers not contained in Infrastructure ENUM may be routed via the PSTN by default. This can be prohibited by using NAPTR RR with the enumservice "void".

The Private ENUM database may be implemented in any DNS domain at the CSP discretion and holds in addition to the information described in the above section also NAPTR RR pointing to the border elements (option 1) or is derived directly from the Public Infrastructure ENUM (in option 2).

These NAPTR RR contain "sip" or "h323" URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. +4319793321@border1.prov.net.



Draft ETSI TR 102 055 (2005-01) - Infrastructure ENUM

Annex I Architectural Models

This section provides a non-exhaustive set of examples of architectures and models which could be adopted, setting out the advantages and disadvantages of each.

In order to highlight the issues, an example confederation with the following parameters is considered;

- Total volume of number ranges : 75,000;
- Size of number ranges : 10K;
- Total theoretical numbers : 750M; and

- Total active numbers : 125M.

Volume of numbers ported: 10%, i.e. 12.5M .

Model A

In a CSP-shared Infrastructure ENUM system the structure of the Tiers is a matter of the participating CSPs. In general it can be assumed that there will be a combined Tier 0/Tier1. The models described here therefore assume that only a Tier 1 is existing on the top level.

If the group of CSPs setting up a shared Infrastructure ENUM decide to use only a database system, the NAPTRs would also be in this Tier and the participating CSPs would provide their data to this database via a common provisioning interface. This structure would be very similar to a centralized NP database.

This would obviously also be the natural model for any CSP-internal Infrastructure ENUM.

Model B

Model B is depicted in Figure BB, and mimics the approach which has been widely adopted for user-ENUM. In this model, the Tier 0/1 contains entries of all of the active numbers, with pointers to the Tier 2 nameservers which contain the actual NAPTRs.

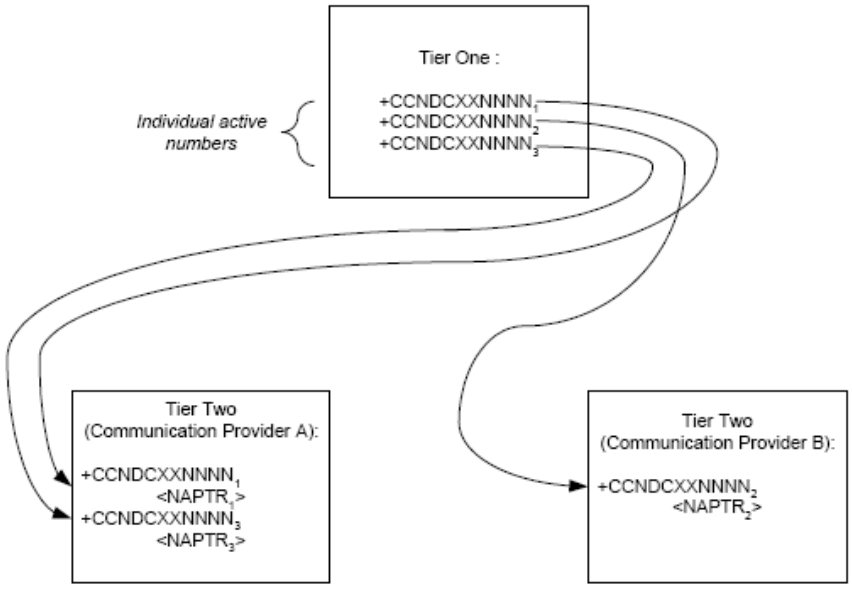


Figure BB : Model B

For the example group, this means that the Tier 1 database would contain 125M entries, relating to each active individual number.

Model B has the large advantage that it readily accommodates number portability in that the authoritative nameserver for each individual number can be entered into the Tier 1. Where the group has adopted an administration approach which requires authentication, right of use of the number can readily be confirmed so long as there is a central number portability database. However, in locations where there is no onward routing solution, it would be impossible to authenticate right of use without

recourse to the donor CSP (e.g. in Figure BB, where the number +CCNDCXXNNNN$_2$ has been ported from CSP A to CSP B, the Tier 1 provider could not confirm this without consulting CSP A).

Model B is probably the simplest architecture where only a limited proportion of CSPs are participating. For example, CSP B could participate without CSP A being involved (excluding authentication issues), which is not necessarily the case for other options.

Set against this, Model B has disadvantages. Firstly, the Tier 1 database must be of a significant size, as it will contain entries for all active numbers: in the example case this means 125M entries. Although this may not cause any technical issues, there may be cost implications for the Tier 1, and participating CSPs will be seeking to minimise the cost of this entity.

Further, this model implies that every time a new number is provisioned, the Tier 1 must be involved in the process to populate that individual number: this may not be acceptable to the participating CSPs.

Where changes are required to the nameserver hosting the NAPTRs for a given number range, it will be necessary to make multiple amendments in the Tier 1 (i.e. an amendment for each individual number).

Model C

Model C seeks to overcome some of the issues around Tier 1 by incorporating all numbers into the Tier 1, whether or not they are active. When a CSP is assigned a particular number range, all of the possible numbers will be populated into the Tier 1, with a default entry of the relevant CSPs. Should any of the numbers subsequently be ported, then the entry against the individual number would be amended to point to the appropriate authoritative nameserver. This architectural model is depicted in Figure CC.

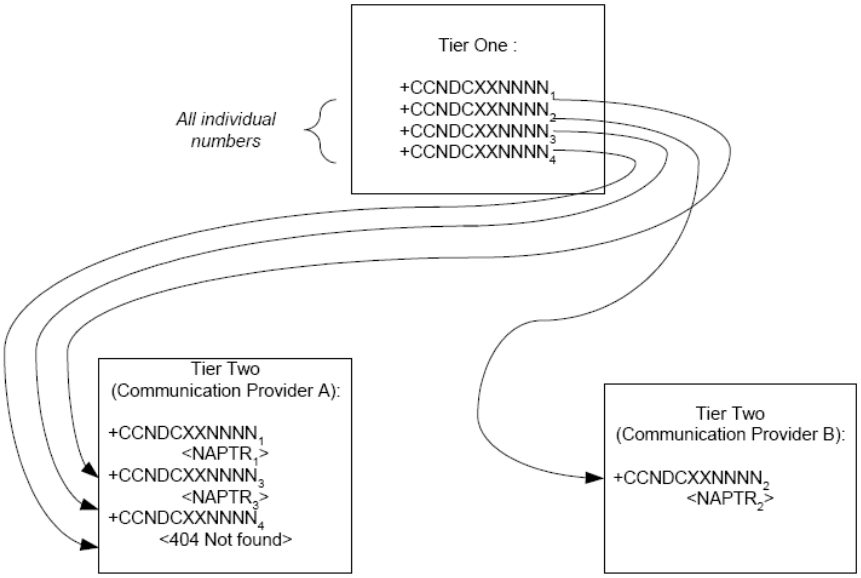


Figure CC: Model C

This model shares all of the advantages of Model B, with the additional advantage that the Tier 1 is no longer involved in the process of assigning numbers to an individual customer.

Set against this, the Tier 1 database will be considerably larger: in the example group, it will contain some 750M entries. This will inevitably increase costs.

Model D

Model D adopts an alternative approach, and seeks to minimise the cost of the Tier 1 function. Rather than be broken out at the individual number level, the Tier 1 database would only contain number range information, pointing each range to an authoritative CSP nameserver. Clearly, this presents an issue with respect to ported numbers: this would be overcome by this nameserver redirecting any queries regarding exported numbers to the relevant recipient CSP's nameserver. This model is depicted in Figure DD.

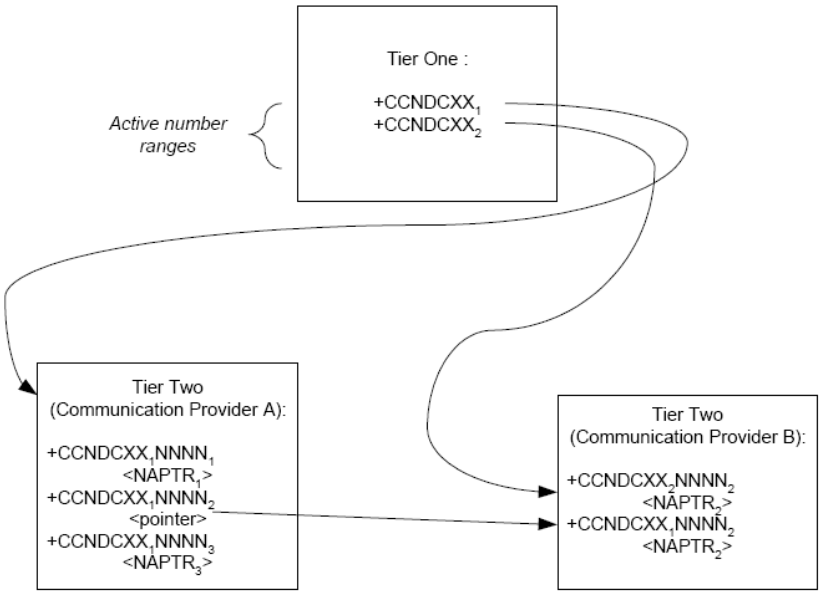


Figure DD : Model D

Model D has the advantage that it minimises the size of the Tier 1 database. For the example group, the Tier 1 database would contain only 75K entries, relating to each active individual number range. In principle, this should reduce the cost of this function.

Where authentication is implemented, then the Tier 1 would have a readily available database to utilise, i.e. typically the numbering database available from the relevant regulator.

The Tier 1 would not be involved in day-to-day numbering administration, i.e. would not need to be involved when a number was assigned to an individual customer. Further, should there be a need to change the nameservers dealing with a given number range, only one entry at the Tier 1 would need to be amended.

Set against this, Model D has disadvantages, largely arising as a result of number portability considerations. Firstly, the model perpetuates the situation where the performance of a recipient CSP is in some way influenced by the performance of the donor CSP, because the latter's nameservers are involved in a query for the former's

numbers. In general, this does not present a practical issue since as portability is a mutual activity, so where B may port from A for some numbers, A will inevitably port from B for other numbers: as such there is an incentive to maintain a reasonable quality of service. However, difficulties can arise where CSPs suffer financial distress: if the donor CSP goes bankrupt, the nameserver will no longer exist to redirect the query. This could be circumvented via a requirement to escrow data from the nameservers in order that a third party could take over operation if this occurs.

Additionally it would be the responsibility of the original range holder to point to the receiving provider when number portability occurs. Whilst this is manageable if the number is first ported, it becomes increasingly difficult with subsequent porting. A user who changes his provider a number of times for whatever reason, would place a heavy responsibility on the original range holder.

Issues also arise in a start-up phase where only a limited number of CSPs are participating. For example, in Figure DD if only CSP B is participating, clearly there is an issue that it is impossible to provision any numbers ported from CSP A. There are two potential ways around this:

a. In Tier 1, entries against CSP A are pointed to CSP B until such a time that CSP A decides to participate. At CSP B's nameserver, only numbers imported to them would be populated, with the remaining non-ported numbers not being populated. Whilst this would retain the small size of the Tier 1, it could present process issues as and when CSP A opts to participate. Additionally, this approach would be complex where another CSP C has imported numbers from CSP A; the implication is that CSP B will need to host both its own NAPTRs and pointers to CSP C's nameserver; and

b. The Tier 1 becomes a hybrid, containing the number ranges for CSP B, and the individual numbers for those numbers exported from CSP A. In the example, in the hypothetical situation where *all* numbers which are ported are ported from CSP A to B (e.g. A is the incumbent), then this would imply that the Tier 1 would contain 12.5M entries. Once again, process issues could arise as and when CSP A opts to participate. Further, it may be the case that the complexity of the Tier 1 will be greater than otherwise will be the case (entries will be of mixed length), thus increasing costs.

Model E

The final model presented in this section is based upon Model D, but seeks to overcome the issues around the performance of a recipient network being dependent upon the performance of a donor. In this model, depicted in Figure EE, the actual nameserver operation is outsourced to an escrow agency.

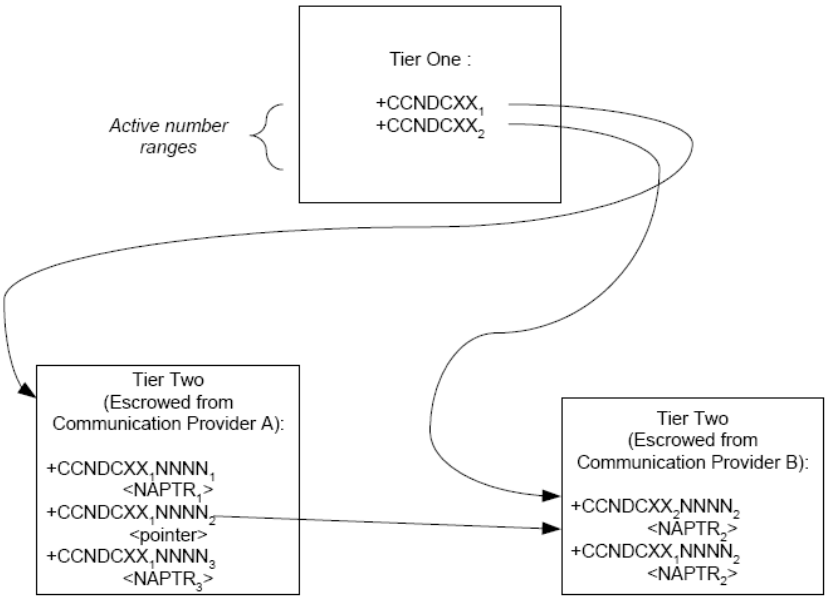


Figure EE : Model E

The advantages of this model are those of Model D, with the addition that a recipient CSP no longer depends upon the performance of the donor CSP.

Set against this, it may not be acceptable to CSPs to outsource the operation of their nameservers. Further, although the recipient is no longer dependent upon the performance of the donor, they are still dependent upon an agency appointed by the donor: it could be argued that this amounts to the same thing. However, there is a difference in that should the donor CSP face bankruptcy, the escrow nameserver would exist, whereas in Model D only the data would be escrowed, meaning it would be necessary to appoint a new nameserver manager and populate the nameserver.

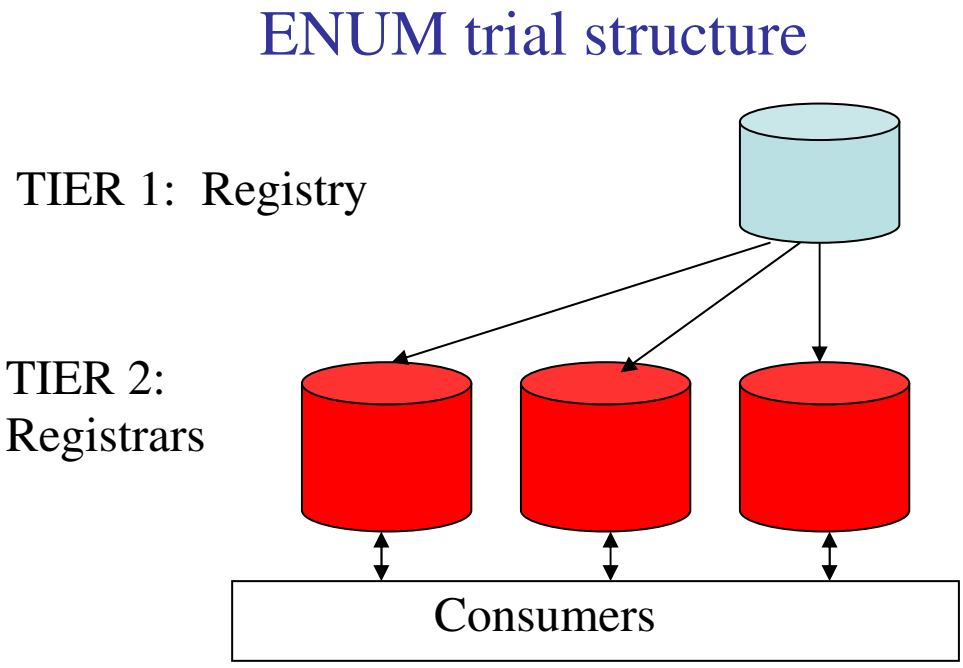
As with Model D, issues arise around any start-up phase where not all CSPs participate. These issues and the potential solutions have been described earlier and additionally the issues with subsequent explained model D also applies.

APPENDIX B: AUSTRALIA

- The Australian Communications Authority (ACA) (now the Australian Communications and Media Aauthority (ACMA))[5] is a government regulator of radio communications and telecommunications. ACA is responsible for developing the numbering plan and administering numbers;
- Industry self-regulation is strongly encouraged, generally through the Australian Communications Industry Forum (ACIF);
- Australian Competition & Consumer Commission (ACCC) is responsible for competition & economic regulation of telecommunications; and
- .au Domain Administration (auDA) is responsible for managing the Australian Top Level Country Code domain.

Implementation of ENUM in Australia

- ACMA is facilitating the process for establishing an ENUM trial in Australia;
- Formed the Australian ENUM Discussion Group in March 2003; and
- The group is a consultative body, comprising members from:
  - The telecommunications industry
  - Internet service providers
  - Universities
  - Privacy and Consumer groups



ENUM trial structure

- Trial will be conducted in three parts.
- This will allow some of the technical aspects of ENUM to proceed whilst policy issues are being resolved.

Part 1

[5] Note that the ACA merged with the Australian Communications Authority to become the Australian Communications and Media Authority.

- This section of the trial will use a new number range: 0590 000 000 – 0599 999 999.
- These numbers will be for ENUM trial use only.
- No connectivity to the public switched telephone network.

Part 2

- Introduction of some existing digital mobile numbers.
- Explore technical and regulatory issues regarding connection between the public telephone network and the Internet.

Part 3

- Introduction of some geographic telephone numbers.

Carrier/Infrastructure ENUM trial update and status

- Trial framework has been established.
- ACA will soon apply to ITU for delegation of .1.6.e164.arpa.
- Privacy guidelines have been finalised.
- Security arrangements for Part 1 of the trial have been finalised.
- Project timeline for the ENUM trial has been proposed.

Privacy guidelines have been finalised

- A WHOIS service will operate for the purposes of technical support, but will not disclose personally identifiable information.
- Registry and Registrars to be treated as 'organisations' under the Privacy Act 1988.
- All personal information collected during the trial to be de – identified once the trial has concluded.
- No additional access to data in the Tier 1 Registry for law enforcement, other than that required by existing laws.

Security guidelines for Part 1 of trial have been finalised

- Part 1 of the trial represents a low security risk.
- Registrant must be contactable by telephone/email.
- Authentication/authorisation is done via a PIN number or password.
- Part 1 arrangements are disposable.
- Industry to develop more robust methods for authentication/authorisation during Part 1 of the trial.

Proposed timing of trial

- ACA to call for expressions of interest for a trial Tier 1 Registry Operator in June 2004.
- Trial Tier 1 Registry Operator selected in July 2004.
- Trial to commence in second half of 2004.
- Trial will run for minimum 12 months, with option to extend for another 12 months.

Important issues to be resolved

Numbering

- Number Plan has to be amended to allow Australian E.164 numbers to be used for ENUM.

Customers' Rights of Use to E.164 numbers and domain names

- Guidelines to be established regarding the contrast in rights of use of E.164 numbers and ENUM domains.
- For example if I no longer have the right to use the telephone number +61 3 9963 6882 then do I lose the right to use the matching ENUM domain: 2.8.8.6.3.6.9.9.3.6.1.e164.arpa.

Authentication & Authorisation

- Secure, online system for validation of ENUM subscribers needs to be developed.
- Current arrangements are only suitable for use with an ENUM-only number range, that is restricted to the Internet.
- Protecting the integrity of the telephone network is a priority.

http://www.aca.gov.au/telcomm/telephone_numbering/enum_nsg2/enum7.htm

Interest in ENUM

- Consumer interest in subscribing to ENUM services.
- Industry interest in committing to an ENUM infrastructure and providing ENUM services.

APPENDIX C: UNITED STATES

Discussion and planning around ENUM has been underway in the United States for some considerable time. The US ENUM Forum began in August 2001 and an ENUM trial finally commenced in February 2006. A limited liability company called ENUM LLC has been established to deliver a Public User ENUM trial. The timeline for this trial is below.

It is worth noting that a number of companies have implemented Private Infrastructure/Carrier ENUM without using any DNS structure. Given the significant issues around privacy and authentication and the stringent rules around use of customer data, many do not anticipate using any other form of ENUM for the foreseeable future.

Country Code 1 ENUM LLC Timeline (as at 31 March 2006)

Date	**Proposed Event**
August 2001	US ENUM forum begins
January 2003	US ENUM specifications approved
April 2003	ENUM Privacy report
August 2003	US ENUM forum re-engaged
October 2004	ENUM LLC (Limited Liability Company) formed
September 2005	Approved letter for CC1 trial ENUM delegation sent to CC1 Governments
November 2005	Two or more CC1 Governments send formal delegation request to ITU to start 60 day CC1 review and concurrence period
February 2006	ITU confirms CC1 trial delegation
March 2006	Formal US Trial Preparation Begins

The following dates are approximate only:

March 2006	LLC releases CC1 ENUM Tier 1A & B draft RFP to US Government
March 2006	Comments requested from CC1 Governments on Tier 1A & B draft RFP
July 2006	Tier 1A & B RFP released to bidders
August 2006	Begin Permanent Delegation Request Process
August 2006	Tier 1A & B Bidder Conference - RFP clarifying questions to LLC
August 2006	Tier 1A & B RFP Responses Due
October 2006	LLC selects Tier 1A & B vendor
November 2006	CC1 Tier 1A & B Vendor Contract Signed
January 2007	CC1 Vendor Tier 1A System Development Completed
February 2007	US Vendor Tier 1B System Development Completed
March 2007	Start 3 to 6 Month Functional & Operational Beta Test
Jun 2007 /Sept 2007	Launch Full Commercial Operations

On the homepage of their website http://enumllc.org ENUM LLC makes the following statements about their approach to ENUM:

"The goal of the Country Code 1 ENUM Limited Liability Company is to build the public infrastructure that will promote the development of ENUM technology in a single, carrier-class manner within the countries of the North American Numbering Plan (NANP). The countries of the NANP include the United States, Canada and the

Caribbean nations."

"We are seeking to build a commercial implementation consistent with the relevant open standards of the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) upon which ENUM is based. The new company will help to implement a single, public ENUM system for those nations within the NANP that choose to participate. It is intended that the North American implementation of ENUM will adhere to national and industry privacy requirements. The LLC's first task will involve selection of a vendor to take the initial steps towards creation of an infrastructure that would enable the countries within the NANP to establish their own national ENUM implementations. The company will also be responsible for selecting a vendor to develop the national infrastructure for the United States."

Trial Type

The US trial commenced in February 2006 to trial Public User ENUM. The document "ENUM FORUM Working Document Requirements for the Implementation of Infrastructure ENUM in the United States" at www.enumllc.org has as its scope to "implement infrastructure (or "carrier") ENUM for geographic Numbering Plan Area (NPA) resources within the US". Note: The FCC imposed 12 conditions on the trial – the most significant of these is that Infrastructure / Carrier ENUM may NOT be trialed. This was an unwelcome surprise to the ENUM LLC as it limits the effectiveness of their trial plans and limits the interest in the trial such that carriers have minimal active input.

Outstanding Issues / Key Assumptions

Some of the key outstanding issues and assumptions in the US are:

- Assumption 1 – "that industry will reach consensus on a specific technical mechanism that allows infrastructure ENUM to be possible. At this point, it is expected that this consensus will be reflected in the appropriate RFC(s) being adopted by the Internet Engineering Task Force (IETF)." At least some of the appropriate RFC(s) are draft only i.e. consensus has not been reached. Note that, given the FCC's refusal to allow infrastructure/carrier ENUM to be trialed, this is unlikely to be achieved;
- Assumption 2 – Standards will continue to develop;
- Issue 1 – Security;
- Issue 2 – Privacy in two key areas. Firstly, the privacy concerns that are inherent in the design of the ENUM protocol itself[6] and secondly, the privacy (and other) concerns that depend on how ENUM is implemented; and
- Issue 3 – Public Policy Issues including administration and control of the Domain Name System (DNS), whether there should be a single "root" for ENUM numbers in the DNS and whether that root should be e164.arpa, and how the "opt-in" requirement (which is the only valid model for ENUM) will operate.

Key Exclusions

- Non-geographic numbering resources are excluded.
- Carrier/Infrastructure ENUM.

---

6 The entire ENUM protocol is based on a simple and unavoidable premise: contact information is stored in the global Internet's Domain Name System (DNS). Because the contents of a DNS record can be accessed by anyone at anytime, any contact information stored in an ENUM DNS record is completely exposed to the world. Thus, to the extent that the ENUM information contains personally identifiable information, ENUM raises a significant privacy concern.

Take-Up

- Nothing commercial to date for User ENUM.
- Private ENUM, not using DNS, is in use in a number of companies.

Observations from US Discussions

The following are points derived from discussions with ENUM strategists under some overall headings.

General

- Carriers want to go with carrier ENUM;
- Trial ends January 2007;
- There are differences between Wired and Wireless. VoIP is NOT the first driver, inter-working for MMS is;
- The technical policy issues are tough – DNS Sec. Very difficult to implement as the standards are "a bridge too far" and no vendor currently supports DNS Sec. Piracy and privacy concerns;
- In mobile will be keyed off the phone number for quite a while (form factor prevents IP address);
- SIP phones have full keyboard but not mobile;
- Presence is a big thing; and
- Everything person to person will have an ENUM hook.

Regulatory / Government

- Regulator / government may prevent Carrier ENUM;
- Little government involvement to date except where necessary (for trial delegation);
- May allow public to piggyback on carrier i.e. infrastructure for carrier and allow public to grow without cost Vs regulated and mud-throwers forcing a path;
- May force a public lookup; and
- Reasonably quiet as the carriers are seen to be doing something.

Business Case

- No business case for ENUM;
- A Limited Liability Company (LLC) established to manage ENUM i.e. not for profit all partners equal shareholders;
- The LLC has been set up in a similar manner to how they manage 0800 numbers – as a central repository for all 01 ENUM numbers. Its major focus is on interoperability and controlling the customer experience; and
- Some see the customer proposition as being the true interoperability service – "it gets to us regardless" and they see it as a way to up-sell and with presence it will be even more powerful. However, customers think of ENUM as FREE.

Number Portability / Numbering

- ENUM may just be glorified number portability;
- The number portability databases and ENUM databases are populated with ENUM information. ENUM data is based on lookup. Some want URLs to be posted in the number portability database;

- May use ENUM as the number portability database. The records are to be static not dynamic and to enable applications.

IMS

- IMS is seen as more important to bring a collection of services including VoIP together;
- One is using IMS for SME VoIP with ENUM as the call routing infrastructure – trial only;
- No inter-carrier IMS standards yet; and
- IMS enables person to person, peer to peer. SIP helps find each other. ENUM is a leg up to routing infrastructure to translate the number to the SIP infrastructure.

Ownership & Public / Private

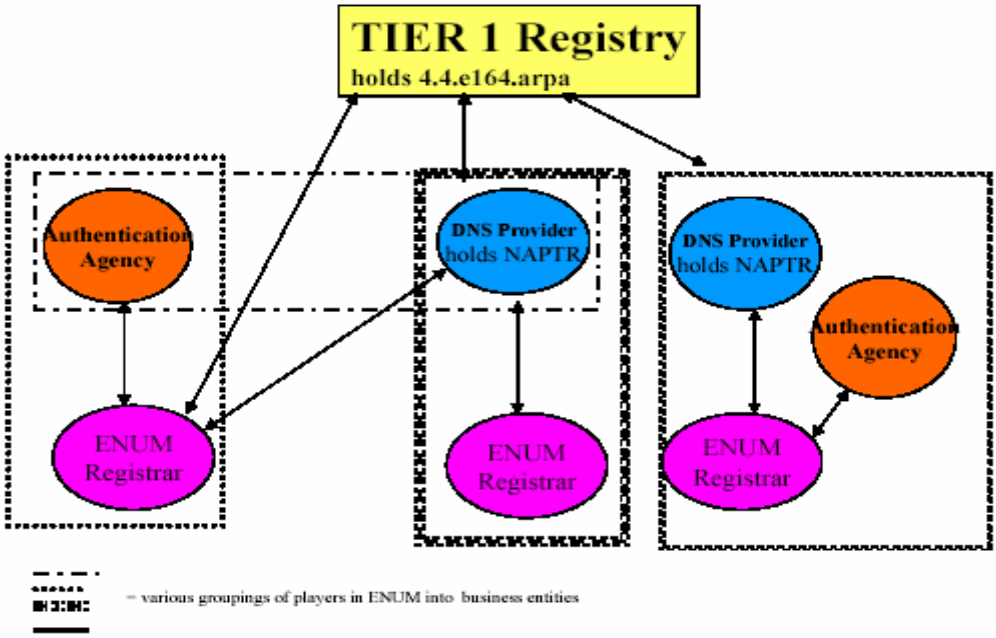
- So far the "ownership" issue has been sidestepped and is not created in the public DNS;
- The privacy argument may prevent the ENUM tree or public DNS; and
- May migrate to the public tree but start using existing i.e. private trees and work with the regulator.

APPENDIX D: UNITED KINGDOM

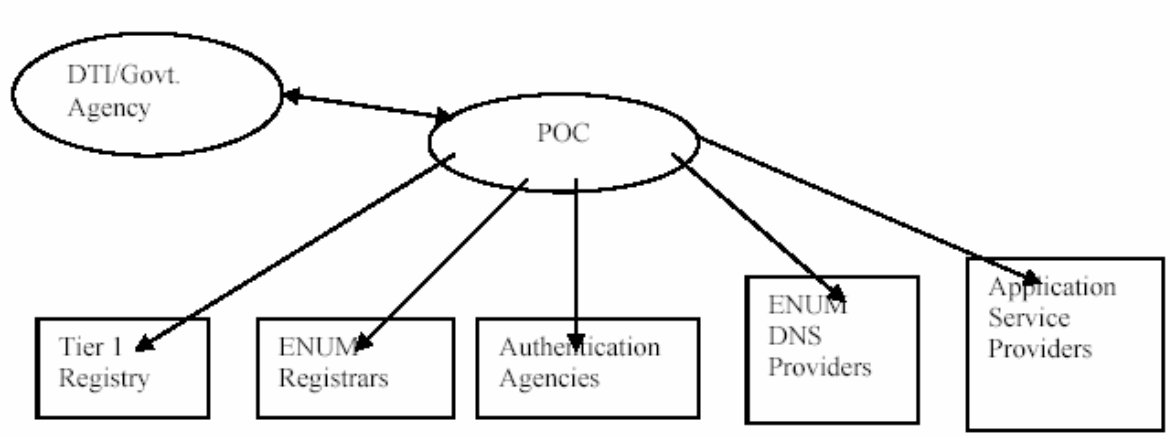
The UK is perhaps one of the most advanced examples of ENUM trials and experience globally. In September 2001, the UK ENUM Group (UKEG) was formed, through facilitation by the Department of Trade and Industry (DTI). UKEG is an ad-hoc cross functional industry group, with representation from Telco's ISPs, registry operators and user groups.

UKEG produced a report [7], focused on User ENUM in April 2002, with one of the key recommendations being to undertake a trial. Other recommendations made in this report included:

- The UK will adopt a policy of 'opt-in' for the UK implementation of ENUM;
- No database will be populated with numbers that are not assigned to end users;
- The UK implementation will adopt all recommendations on consumer protection and data privacy in line with guidelines and best practice as advised by the Information Commissioner's Offices;
- ENUM applications must ensure that the existing requirements for number portability are retained;
- In principle any UK number range can be included in ENUM;
- The UK will implement a single Tier 1 Registry architecture serving all UK E.164 numbers;
- NAPTR records will be stored in the ENUM DNS Provider's database;
- The UK will implement an architecture at Tier 2 that will allow entities to provide one or all of the following services: ENUM Registrar services, DNS Provider services, AA services;



- The role of a Tier 1 Registry is best carried out by a single entity as opposed to competing or multiple entities. Competition in ENUM services is proposed to take place at the ENUM Registrar level;
- The UK should create a Policy Oversight Committee for UK ENUM; and



- The selection of the Tier 1 registry for the UK should take place using an open, public and transparent process and selection based on the criteria proposed, together with cost and experience.

A UKEG Trial Seminar was undertaken in September 2002, a trial pack issued and request for "expressions of interest" sought. The first meeting of the trial group was in December 2002 and work began on the trial in January 2003.

The aim of the trial was to test architectural, technical, operational and user experience aspects related to the provision of ENUM capabilities for country code 44.

The UK ENUM trial successes included:

- Agreement on the top level model, roles and responsibilities;
- Substantial progress on authentication and accreditation;
- Process requirements defined;
- Criteria, principles and interfaces developed; and
- Issues over delegation procedures dealt with.

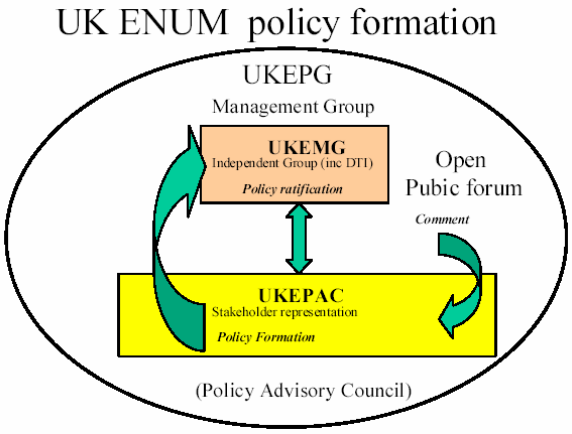
The major issues emerging from the UK ENUM trial included [8]:

- **Authentication** - The process of identification and validation is a critical element required to protect end user privacy and data integrity. Only authorised number assignees should be able to subscribe to, change or cancel their ENUM registrations. One of the key issues is that there is no central database to authenticate against. Long term solution likely to be based around UK number portability process. TSP (Telephone Service Provider) participation is highly preferred, given their strong background in this area. Another possible 'trusted' solution is a PIN mailed to registered address. A more 'basic' authentication method, used as a final fallback, could be the presentation of supporting documentation e.g. bill, bank statement with passport, or driving licence.

- **Policy formation** - a key requirement identified by UKEG was that 'policy development has to be open, fair and transparent'. Who should develop policy and on what basis? DTI has stated 'they will not assume this responsibility'. Who will make the rules? How will they be implemented? What powers will

[8] ENUM - An Introduction, Tony Holmes BT, NAD Management Committee & Internet NZ Seminar, Wellington, 24 November 2003

exist? UKEG has considered the initial problems and identified a possible way forward:



- **Tier 1 Selection** - Selection of a single Tier 1 Registry means somebody must assume overall responsibility, somebody has to make the choice. DTI has stated 'they will not assume this responsibility'. UKEG has recommended an "open competition for Tier 1 Registry". UKEG have developed basic principles for registry operations covering operational and technical requirements, business, financial, legal and other requirements and developed a criteria assessment document.

- **Separate number range?** - Has been discussed. Could provide early recognition of 'ENUMbers'. Possible network benefits. No conclusions yet.

In August 2004, DTI undertook a consultation process on the proposed arrangements for ENUM. The results of this consultation were published in April 2005. The three main issues that the DTI consulted on were:

- The proposed implementation of ENUM in UK including the distinctions in the functions between the single Tier 1 registry and the competing Tier 2 registrars and nameserver providers;
- The management arrangements for ENUM including the formation of the UK ENUM Committee and the principles for the appointment of the Tier 1 registry and the terms under which the registry will be run; and
- The arrangements for the authentication ENUM entries.

The consultation endorsed the plans of the UK ENUM Group for the structure and different functions for implementing ENUM and the process for the appointment of the Tier-1 Registry. The Consultation endorsed the views of the participants in the UK ENUM Group that the validation and authentication of ENUM entries is of the highest importance as are the issues of privacy and the prevention of SPAM in its many different forms.

The following are the main issues identified through the consultation as needing further study if ENUM is to be "brought to market" successfully:

- Refining the validation and authentication process so that it provides adequate security and yet does not become a major barrier to people entering their data into ENUM;

- Ensuring that data in ENUM is accurate and up-to-date and that ENUM entries are deleted when service on numbers is ceased;
- Ensuring that there is adequate subscriber awareness that data entered into ENUM will be open to the public;
- Clarifying issues concerning ENUM entries for numbers that are shared;
- Ensuring that premium rate numbers do not lead to abuse in ENUM;
- Developing more ideas for applications based on ENUM;
- Finding ways to motivate users to enter their data into ENUM to build critical mass; and
- Preventing abuse of the system, ensuring it develops for the public benefit and that these issues are adequately protected within the organisational structure of ENUM.

The report also outlined the Government's policy for the further development of ENUM, with the expectation that this will be largely led by the commercial sector.

APPENDIX E: NETHERLANDS

The *Directoraat-Generaal Telecommunicatie en Post* has published in April 2001 a document[9] on the principal considerations on ENUM and the approach in which the Netherlands could collaborate in the implementation of ENUM. The most significant aspects of this document are:

If the ENUM discussion takes too long, there is a risk of taking a decision without consensus of all concerned actors;

- Certain numbers are distributed to multiple users, a new numbering plan has to be contemplated (ENUM number range);
- The data in the ENUM database always have to be updated; this is an indispensable service for the database manager.
- They agree with the Swedish position on the necessity to guaranty public services, *conditio sine qua non* for the European telecommunications operators. No monopoly should be allowed, the proposals tend to this situation; independent organisations should develop rules in users' interest terms and free market. The idea of competition is absent in the present proposals.
- Consider price control, in order to avoid the fact that services would be proposed at too high prices, preventing the development of the system. Consumer protection has to be fundamental in the implementation of ENUM; access to data in the ENUM base could attend to the privacy of the users and precautionary measures should be put in place. The security aspect is not developed in the documents published either the IETF, ITU or ETSI in relation to ENUM.
- The DGPT has reserves on the co-existence of national TIER-1 and commercial TIER-like's in terms of number portability and coherence and interoperability of associated services. However, it is difficult for the regulators to prevent the creation of private alternative ENUM systems: the market advances at a different pace than the ITU (189 members have to agree).
- The proposed management structure (TIER-1 and TIER-2) has a potential weakness due to the distributed nature of the solution; co-ordination, implementation and selection of around 200 ITU members could be a disadvantage for a service, which demands before all coherence. The risk is to uphold the development of the applications.

APPENDIX F: FRANCE

The "Secrétariat d'Etat à l'industrie" and the "Autorité de régulation des télécommunications", responsible for the national numbering plan, launched a public consultation (May-June 2001) on ENUM, in considering the fact that the issue exceeds largely the strict French management and regulatory frame. On 16th of July 2001 the ART published the results of the public consultation on the principles and conditions for implementing the ENUM[10] protocol.

A number of doubts exist on the ENUM proposals made to this day.

It is essential to limit the management of the ENUM domain names to numbering in order to preserve the coherence of systems and to assure the appropriation of services by a large public.

This choice, which is not confirmed yet, instigates a controversy on the fact to insert a national European numbering plan under a domain controlled by the US government (via ICANN).

The uncertainty on the choice of the reference domain of the ENUM names doesn't have to withhold a fast definition of transparent management rules for the delegations nor hide a debate on this question, which in reality constitutes its principal challenge.

Proposals exist on the possibility to let parallel TIER-0 develop (ex: "gprs" for mobiles) and trust market mechanisms to decide between different systems.

In this context it is possible to foresee that multiple systems of the ENUM type will develop, like for the TIER-1 commercial companies Verisign and NetNumber. However in this case incoherence in numbering and also neutrality, the reliability and the national coverage are at risk.

The role of co-coordinator in the implementation of ENUM has to be given to the ITU to ensure system coherence with the E.164 numbering plan. The ITU also has to control the delegations of sub-domain databases to guarantee that a State is reserved the delegation of the management of the TIER-1 correspondent to its national code.

The ITU could also define certain essential insertion rules for the numbers in the DNS on the supra national level. This would allow a management of ENUM resources independent of market actors.

From the proposals made, the management of the TIERs should be the following:

TIER-0: in the case of E.164 it is preferable that it would be the ITU-T.

TIER-1: the governments are responsible for the domain corresponding to their country code(s), and appoint a responsible entity for the management of their subdomains; a TIER-1 entity is equal to a "ccTLD" registry.

TIER-2: it will be the responsibility of the organization that manages the registry of the final user numbers in the domain TIER-1; this level corresponds to the Internet domain names, with the Internet Registrars. Besides the registering of the numbers

in domain names, TIER-2 maintains a database where each name in the ENUM domain is associated with the communication services allowing to access the final user. An ENUM domain name has to be recorded by a unique TIER-2 service supplier (to avoid incoherence during the resolution of a DNS request).

TIER-3: is managed by the communication service supplier. The database of a TIER-2 service supplier refers to the service suppliers' server (bridge for telephony over IP, message server, etc.)

The managers of the TIER-2 and TIER-3 prevent cybersquatting.

A risk exists in the fact that only the manager of the ENUM base is capable of supplying ENUM protocol services.

The supply of telecommunication services is subject to obligations (ex: channelling of emergency calls, legal interception of calls, universal service financing, etc.); those aspects are not considered in the present management hypotheses.

APPENDIX G: SWEDEN

The PTS (Post and Telestyrelsen, the national agency for post and telecommunications) has been charged by the government to analyse the possible collaborations in the implementation of ENUM in Sweden; a document (01-9734)[11] has been published in March 2001.

The principal points of this text are the following:

According to the IETF documents the TIER-0 responsibility will be delegated to IANA-ICANN; this has not been approved by the ITU whilst the Internet world (IETF-IAB) seems to push in that direction. The proposals to create different parallel TIER-0 have to be discussed in order not to create incoherencies in the supplied services. The different positions have to be clarified as soon as possible before any ENUM services are put in place.

Certain states, including Sweden, are reluctant to accept the management of TIER-0 by an organization linked to the US government; however, with the guarantees offered by the ITU-T "arpa" management, consider this as the best choice.

The management of the TIER-1 has to be ensured by the states following their request to RIPE-NCC; however, the creation of commercial TIER-1, for ENUM-like functions (ex: Verisign, NetNumer), could create incoherencies in supplied services to the public and in the interoperability of the two systems. Moreover, the upcoming situation could result in a risk to create conflicts between ENUM-like commercial services and those of the national regulatory authority, which are submissive to constraints.

This is the reason why the PTS recommended that the government make a rapid decision, before ENUM-like services are developed.

The PTS considers that the government should delegate the organizational management of the national TIER-1 to them and that the management of the TIER-2 should be given to an independent ENUM service supplier, which offers services and portability guarantees.

A 12-month trial period must guarantee the service reliability and will be useful to show the weak points and to resolve the problems. After this period, an in-depth evaluation has to be realised by the government.

APPENDIX H: AUSTRIA

2001	First Consultation from RTR (the Regulator)
2002	RTR Workshop Austrian ENUM Trial Platform (AETP) formed Delegation from RIPE NCC in May ENUM Trial in operation in September
2003	New Telecommunications Act in conformance with EC Directives ENUM Trial ongoing Discussion of admin and legal issues in AETP
2004	New Numbering Ordinance (KEM-V) Contract between RTR and nic.at Commercial service opened in December
2005	ENUM enabled number range 780 opened in May

Lessons learnt in Austrian ENUM Trial

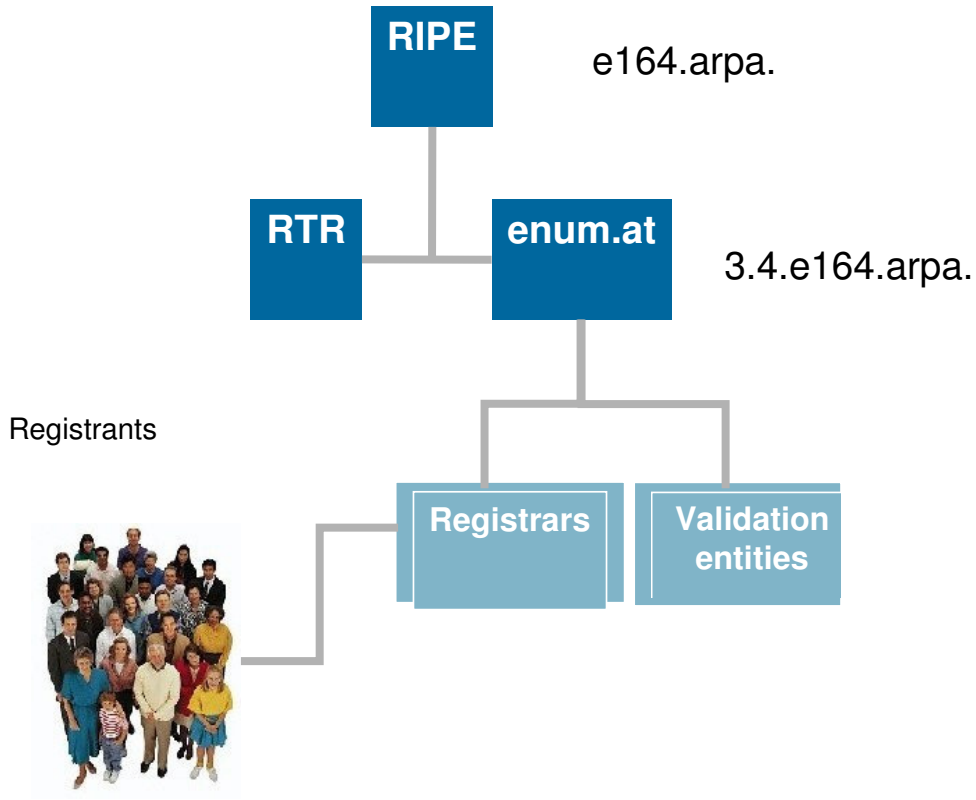
The Austrian ENUM Trial Platform fulfilled its task:

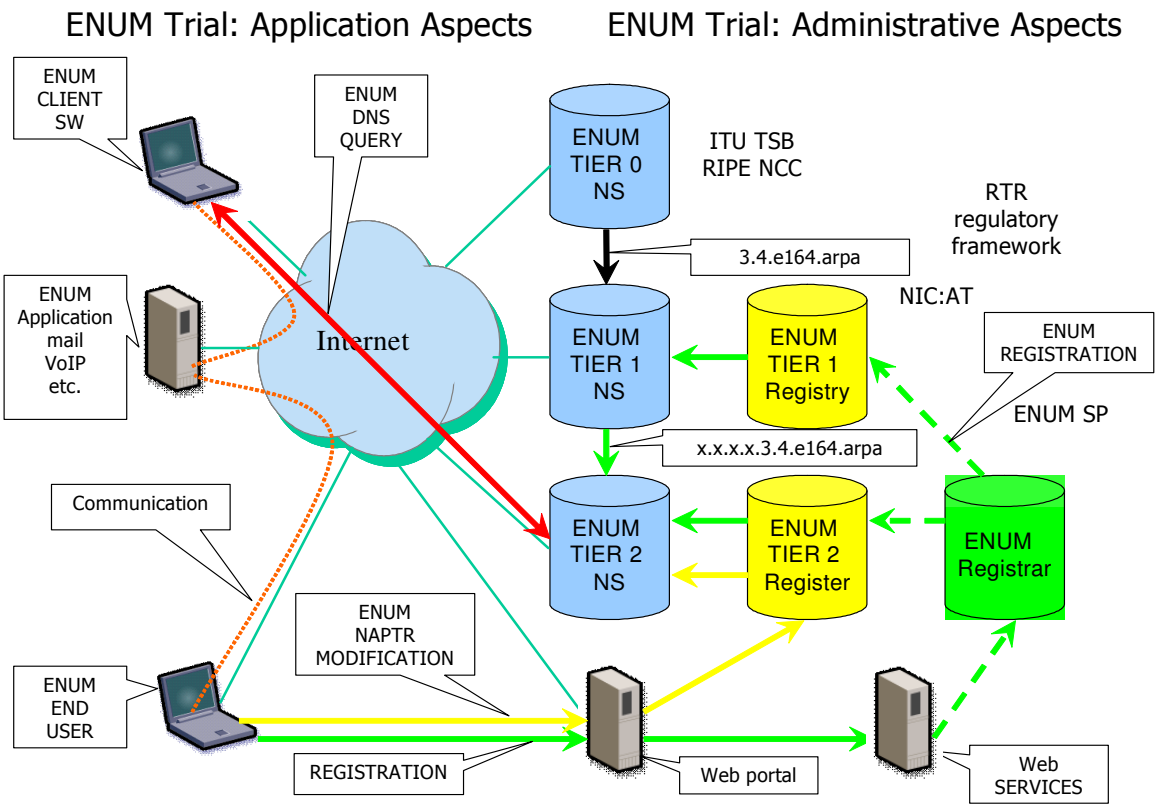
- demonstrated the feasibility of ENUM (proof of concept);
- provided examples of lessons learnt;
- highlighted the open issues (e.g. validation, numbers to use);
- regards User ENUM ready for production with operator accountability to protect PSTN number range integrity;
- It was necessary to embed ENUM in the legal framework;
- This is done by the Austrian National Regulatory Authority (NRA) – RTR;
- Privacy concerns reduced the usability basically to VoIP only;
- BUT most VoIP providers do not provide end-users with SIP URIs to be reached on the Internet without termination fees;
- Why should an end-user pay for the benefit of other users? and
- Few people outside the industry understand ENUM.

Basic issues solved:

- ENUM naming and routing technology works;
- ENUM policy and administration: problems are solvable;
- but there was a shift in focus for the business models;
- The original business model of ENUM for residential subscribers with opt-in for existing numbers has problems;
- limitations exist so ENUM may assume second line service;
- privacy problems with multiple services (e-mail spam);
- no real-time re-validation mechanism exists making available identity theft techniques a real subscriber threat;
- The basic idea of ENUM has some draw-backs;
- Basic Lesson: – you cannot sell ENUM; and
- You can only sell a product or a service (application) so new approaches are needed.

Registry Architecture in Austria





User Cases for ENUM during Austrian trial

a. Business: IP PBX and IP Centrex
   - with geographic and/or numbers for networks (ENUM opt-in)
   - linking VoIP islands together globally via the Internet
   - will be reached from the PSTN via private or public gateways

b. Residential and Business: ENUM-driven numbers
   - IP device can be reached from IP and PSTN (via generic gateways)
   - calls may be routed to IP directly from the originating PSTN network

c. Residential: mobile numbers (ENUM opt-in)
   - terminate IP originated calls on IP, plus eventually forwarding or forking to the mobile phone
   - PSTN operators may provide forced ENUM access from the PSTN via GG

d. Residential: geographic numbers (ENUM opt-in)
   - secondary line (separate termination on PSTN and IP)
   - primary line attached via terminal adapter or SIP-server with FXO port
   - primary line (ported out), reached from PSTN via Point of Inter-connect

APPENDIX I: CANADA

The Canadian Steering Committee on Numbering (CSCN) recommends the following approach be used to address the evolving ENUM issues (during and after) an ENUM trial:

a. There is a need for a single entity to perform the Tier 1 ENUM functionality to serve all the nations in the country code 1 NANP area that elect to participate in ENUM, for two reasons, namely that some NANP NPAs are used to provide telephone numbers to customers in more than one NANP area country (e.g., toll free NPAs), and that some NANP area nations may wish to control the provision of their own Tier 2 ENUM functionality and vendors.

b. The location of the Tier 1 ENUM registry for Country Code 1 is to be determined based on government policy, business and technical factors, including:

- responsiveness to the regulatory and legal requirements of all NANP nations including Canada;
- cost to perform this function;
- prices for Tier 1 Registry services to be charged to Registrars, Tier 2 Registries, Tier 2 Registry Providers and Registrants;
- convenience to Registrars, Tier 2 Registry Providers and Registrants, including operating hours;
- response times, percentage of time service will be interrupted, failure rates and other matters pertinent to service level agreements;
- responsiveness to the requirements of Registrars, Tier 1B Registries, Tier 2 Registry Providers, and Registrants (including dispute resolution); and
- such other factors as may be identified by reference to existing domain name registry and telephone numbering operations.

c. The Tier 1 Registry function for Country Code 1 should be provided by an entity selected and agreed by the national regulatory authorities of the nations participating in ENUM in Country Code 1. In the case of Canada being a regulated market, the federal Department of Industry and/or the CRTC would perform this role, with inputs from the Canadian ENUM participants. The CSCN also submitted that interested parties from all NANP nations should have the opportunity to submit comments and participate in the process for the establishment of the requirements, selection and governance of the entity to which the 1.e164.arpa TLD would be delegated.

d. The Tier 2 ENUM Registry function for Canada should be performed by a vendor that is acceptable to the Government of Canada and Canadian ENUM participants. The choice of a Tier 1 vendor for Canadian ENUM numbers should be made by either the Canadian government or a Canadian ENUM industry organization established for this purpose (e.g., the CSCN, a CISC Ad Hoc Committee, a Canadian ENUM Consortium, etc.). The process for selecting a Tier 2 ENUM vendor for Canada needs to be investigated further, based on policy and direction which the CSCN invites from the Government of Canada.

e. The Tier 2 ENUM Registry function for Canada should be performed by an entity that submits an acceptable proposal in response to an RFP that defines the Canadian ENUM requirements. This vendor could be the same vendor

selected by the USA ENUM LLC to perform Tier 1 ENUM Registry functions for the USA and other NANP area nations, or a different vendor to perform the Tier 2 Registry function for Canada.

f. Under the ENUM Forum Specification, the Tier 2 Registry Provider level would be “competitive” as multiple vendors could compete to provide Tier 2 Registry Provider services to Registrants. Multiple Registrars would compete to provide the registrar service functions. An individual entity may be a Tier 2 Registry Provider, a Registrar or both a Tier 2 Registry Provider and Registrar. To ensure a fair competitive marketplace for Registrars and Tier 2 Registry Providers, the entities selected to perform the Tier 1A and Tier 1B functions would not be permitted to be a Registrar or Tier 2 Registry Provider.

The CSCN should investigate and propose a funding mechanism for paying the costs of operating the ENUM system including the costs of the Tier 0, Tier 1 security mechanisms, and Tier 2 Registry administration. The costs should be recovered from those who use, benefit from, and provide ENUM services. A cost sharing formula will have to be developed and either agreed by all participants and/or submitted to the CRTC for resolution and/or approval.

APPENDIX J: UK ENUM Trial Group (UKETG) Report May 2004

Accreditation for UK Production ENUM

Introduction

The question of accreditation for parties involved in UK ENUM has been around for some time and discussions to date have been fairly brief and inconclusive. The UKEG report to DTI covered the issue briefly under section 10.2.1, which stated:

'Consideration has been given to which, if any entities would need accreditation, and if so who would carry out this function. It is clear that the Authentication Agency (ies) would require accreditation, and that the ENUM DNS Providers would not require accreditation (given they are carrying out a "vanilla" DNS function). However, the position is not clear for ENUM Registrars.

The advantages of accrediting ENUM Registrars are as follows:

- By accrediting ENUM Registrars, the Tier 1 Registry can effectively treat them as a trusted party, in absence they would have to be treated as an untrusted party. As an untrusted party, the ENUM Registrar would have to provide validation information from the AA to the Tier 1 Registry in each communication, implying that the Tier 1 Registry would have to check this. This would imply additional (albeit small) functionality at the Tier 1 Registry - as this is a monopoly this is arguably inefficient; and
- Without accreditation, only the Tier 1 Registry would be considered to be trusted, meaning that functions around monitoring when the "subscription" on a given number was due to expire and initiating the removal of that subscription in absence of a renewal, would have to be carried out by the Tier 1 Registry. As with the previous bullet, arguments around monopoly efficiency point to limiting the role of the Tier 1.

Set against this, the principal disadvantage of accrediting ENUM Registrars is that some form of accreditation regime would be required, raising questions of who would accredit, against which criteria, with what legal basis and so on. A decision has therefore not been reached, and the issue will be explored during the trial.'

The aim of this paper is to take the accreditation issue forward from this position and to make proposals regarding accreditation for the production stage of UK ENUM that can be considered by the industry and its stakeholders as part of the planned DTI consultation. It is assumed that any accreditation scheme would be developed with both industry and stakeholder input, with the aim of achieving consensus as to a way forward.

ENUM-Exchange

The insertion of E.164 numbers into ENUM services requires a verification process to protect subscribers of E.164 numbers from having their numbers input into ENUM services without their permission.

In the UK Ofcom allocates numbers for operators to assign across their networks. These operators or carriers (in telephone language) expect and are expected by their customers and Ofcom to be responsible for the telephone services provided to their subscribers.

The management and performance of telephone numbers is an important aspect of this service.

Therefore it is important that a verification process is conducted to ensure that a telephone number when inserted into the DNS is done with the subscriber's permission.

However for a mass market deployment of ENUM the process needs to be conducted in a simple, secure and low cost manner whilst still offering sufficient public safeguards.

The decentralised nature of the DNS means it is neither possible nor desirable to centralise this service for all customers of UK telephone services, nor is it possible or desirable to require all carriers to either provide ENUM services themselves or act as verification or authentication agents should they not wish to do so on behalf of their and other carriers' customers. Likewise customers may use several carriers and wish to consolidate their ENUM provision through a single ENUM service.

It is important for all customers of telephone services should they wish to be able to register their E.164 numbers into the DNS to be allowed to do so irrespective of any carrier's commercial interest in ENUM. It needs to be understood that it is not in the power of a carrier to prevent a customer from registering a number in ENUM. However it is recognised that it is not desirable to register E.164 numbers without taking care for the bona fide interests of the number's owner/user.

Verification remains necessary but it need not necessarily require input from the carrier. Naturally verification by the carrier offers the highest level of verification possible in the circumstances of E.164 numbers and so would naturally be a preferred method.

UKETG must describe a structure to promote an open market for provision of ENUM services. Key to this structure is the development of a tier of Authentication Agencies also described as Verification Agencies whose duty is to receive an application for ENUM provision and to verify that the application and its Registrant and telephone number match and so can be input into the UK ENUM database at *4.4.e164.arpa*. An ENUM registration will cause the Tier 1 Registry to delegate the corresponding domain to the name servers chosen by the Registrant. This domain can then be populated with NAPTR records or anything else considered appropriate. How this is done and how the name servers are provisioned is a matter of customer choice.

Due to the variety of ways that verification might occur, and the sensitivity of the information, the role of verification or AA requires a significant level of trust between the various agencies often in a competitive environment. Also, good conduct and practice in regards the management and disclosure of such information needs to be safeguarded to give confidence that the broad range of verification techniques deployed are being done responsibly.

It is envisaged that such confidence can be built through an accreditation mechanism to be applied to verification / AA. A self-regulating clearing system or exchange is suggested where businesses join by agreeing to standard of operation, liability, responsibility and minimum knowledge in their participants in order to transact and verify ENUM registrations.

Certain advantages also accrue to this type of approach from a commercial standpoint. By establishing an exchange format it enables a closer co-ordination between the telephone and Internet operators and this is likely to both deliver better understanding and so facilitate services and revenue opportunities between the two sectors. Secondly the verification process involves a small but identifiable service to provide a reasonable verification for the insertion of an ENUM entry. For this a fee is likely to be a fair recompense to those providing this verification.

Whether a verifier chooses to charge the Registrar making the verification request or if a carrier their customer or both, the provision of verification represents a financial value, which is needed as a market mechanism. Likewise customers require adequate protections through competition and adoption of common market practices available in an open self-regulatory regime.

The establishment of an ENUM exchange where such activities are conducted openly offers a structure where these issues can be developed to meet both public concerns and business needs. It may also offer significant ways to keep prices low to stimulate the market through addressing market efficiency mechanisms such as financial clearing services between participants.

Accreditation Aims

As noted above, there are potential issues of consumer trust and confidence in ENUM. There is also a perceived need to differentiate from previous “scams” and to ensure government and regulator confidence.

However, if there is to be any form of accreditation, it is important that it is well thought through and agreed by the stakeholders involved. It is essential to ensure that any agreed standards are really required and set at an appropriate level, in order to comply with competition legislation, for example. Standards that exceed these levels, whilst they might be desirable by some, would potentially limit the number of potential participants able to meet those standards.

In order to address potential issues from the Registrant’s point of view, areas such as pricing clarity, service levels, advertising, data protection, moving from one Registrar to another etc. will need to be covered, either contractually or by accreditation.

There are also potential issues regarding AAs and TSPs, and co-operation between organisations in these roles and the avoidance of avoid anti-competitive and monopolistic practices will also need to be addressed.

Types of Accreditation Models

Although the term accreditation has been used previously, it is useful to explore the available options. As there has been widespread support for some sort of accreditation for UK ENUM, the uncontrolled option has already been ruled out.

The options are as follows:

- Accreditation by examination – where organisations wishing to act in a particular role would need to apply and pass some sort of examination or formal assessment to be officially authorised to do so, prior to acting in this capacity. Accreditation breaches could be dealt with by complaint and there could also be periodic re-examination or external assessment;

- Accreditation by self certification – where organisations wishing to act in a particular role would self certify that they would meet the requirements, prior to acting in this capacity. There would need to be a complaints scheme for alleged breaches of the accreditation;
- Voluntary code of practice – where organisations can choose to agree to comply with a code, but do not need to do so in order to act in any capacity. This would also require a complaints scheme; and
- Case based self-regulation – where there is no code of practice or accreditation. Complaints are considered on a case-by-case basis by an impartial group, which determines appropriate responses.

Accreditation Scheme for UK ENUM

There was agreement that, no matter which accreditation scheme is chosen, there will need to be a complaints process by which alleged breaches can be dealt with and appropriate sanctions made available. In view of discussions regarding the governance of UK ENUM, it is proposed that this process would be the responsibility of the UK ENUM Policy Group.

There then remains a decision regarding which type of accreditation model would be most appropriate for the UK ENUM industry.

It is considered that accreditation by a voluntary code of practice could be fast and cheap. If the scheme could achieve a high profile, it could also be very effective. However, it could potentially lead to two tiers of provider – those who had elected to comply and those who had not. It is thought highly likely that the reasonable providers would join such a scheme and rogue providers would not. It is assumed that scheme revenue would be provided by those who had elected to join it, and would be mainly used to raise user awareness. Without high user awareness of the risks of using a supplier who was not a member of the scheme, this option could well lead to user confusion and the lack of a process or remedy to address complaints made about suppliers who were not signed up to the code, but who were alleged to be in breach of it. It is considered that these risks outweigh the benefits of this type of accreditation.

A case based scheme, with any complaints considered by an impartial group, could offer flexibility and possible low costs. However, the lack of agreed standards at the outset would necessitate standards being developed over time, by case law which could result in inconsistencies and lower standards that would be set by an agreed code of practice. It is considered that these risks outweigh the benefits of this type of accreditation.

It is considered that accreditation by examination or some other type of formal assessment would potentially be comprehensive and give a high level of certainty that the accreditation requirements had been met. However, this could also potentially be costly to applicants resulting in a barrier to entry, bureaucratic in that a comprehensive audit trail may result/be required and there could also be delays in applicants becoming accredited. It is considered that these issues outweigh the benefits of this type of accreditation.

The remaining option is accreditation by self-certification. This is considered to be the preferred method of accreditation for UK ENUM, where the standards for the scheme would be set by industry and stakeholder consensus and the costs of the scheme would be met by those seeking accreditation. The process of accreditation would be quick and cheap and there would be a complaints scheme for alleged breaches. There is a risk that the costs of the scheme and the levels of service/competence etc for accreditation could create a barrier to entry and this would need to be taken into account when devising the scheme. However, it is considered that this risk is outweighed by the benefits of such a scheme.

Scope of Accreditation

It is assumed that the conduct, procedures and practices of the Tier 1 Registry will be covered by a contract and that problems relating to any of these would need to be dealt with by the Policy Oversight Committee or their equivalent.

It is also assumed that there are some parties in UK ENUM that it may not be appropriate or necessary to accredit, such as Registrants, DNS service providers and application service providers. Therefore, some form of accreditation may only be appropriate for ENUM Registrars and Authentication agencies.

It is further assumed that there will be a series of contracts between the key roles in UK ENUM and that a number of common issues, for example: security, data protection and technical standards etc may well be defined within those contracts. The contracts will be under UK law and will also need to incorporate provisions for Registrars and other entities that are based outside of the UK.

It is therefore recommended that the roles of Registrar and AA should be accredited for UK production ENUM.

Roles to be Accredited

<u>Registrar</u>

A Registrar will have a commercial relationship with an ENUM Registrant and with an AA (or more than one AA). A Registrar will need to:

- Collect the information required by AA and Registry including collecting and returning validation data (PIN Codes) to AA where required - i.e. the Registrant may not send this data directly to the AA;
- Possibly carry out validation (or attempt to) to the AA's requirements;
- Deal with the Tier 1 Registry as an agent for the Registrant;
- Provide support services in relation to the ENUM registration to the Registrant, including facilitation to an alternative Registrar if requested by the Registrant;
- Ensure that DNS servers and requested delegations meet required technical standards;
- Comply with data protection and privacy legislation and best practice;
- Ensure that aspiring Registrants are aware of all relevant terms and conditions and charges when making a registration;
- Ensure that all of their customers are provided with Registrar contact information for any queries or problems with their registration;
- Operate a complaints procedure;
- Comply with the requirements of any agreed accreditation scheme; and

- Ensure that any resellers of the Registrar comply with all relevant elements of the Registrar's contract role and any accreditation scheme.

Authentication Agency

An AA will have a commercial relationship with one or more Registrars and will need to:

- Be responsible for ensuring validation and authentication is carried out to agreed standards and within acceptable timeframes;
- Be able to make authentication & validation enquiries to any participating TSP;
- Possibly outsource parts of the validation process to Registrars under a commercial arrangement;
- Comply with data protection and privacy legislation and best practice;
- Operate a complaints procedure; and
- Comply with the requirements of any agreed accreditation scheme.

All AAs must be equal as far as TSPs are concerned and an AA does not have to be a telco, although a telco may also be an AA.

Responsibility for Accreditation

It is proposed that responsibility for accreditation will need to rest with the UK ENUM Policy Group or some other relevant body within the UK ENUM governance framework. They may, in turn, delegate the management of the scheme to an appropriate and competent organisation.

If the scheme is managed by the UKEPG, work would need to be delegated to a secretariat (the UKEPG may need a secretariat anyway), and it is likely that there would need to be some sort of sub-committee involvement with complaints etc, depending on the accreditation model decided upon.

There is also the possibility of using existing relevant accreditation frameworks, such as the Telco Charter, which may be appropriate for AA accreditation.

Recommendations:

Registrar Accreditation

That all UK ENUM Registrars will be required to join an accreditation scheme and that entrance to that scheme would be by self-certification. Once self-certification has been completed, the Registrar will be known as an Accredited UK ENUM Registrar. The Tier 1 Registry for UK ENUM will only accept registrations from Accredited UK ENUM Registrars.

AA Accreditation

That all UK ENUM authentication authorities will be required to comply with a scheme of accreditation approved by the UK ENUM Policy Group. Once compliance has been self-certified, the AA will be known as an Accredited Authentication Agency. UK ENUM Registrars will be required to use Accredited Authentication Agencies for all UK ENUM validation and authentication.

Accreditation Scheme Oversight

The UK ENUM Registrar accreditation scheme and the AA accreditation scheme is the responsibility of the proposed UK ENUM Policy Group.

UKEPG Tasks

UKEPG should establish any necessary accreditation schemes. This would entail developing the procedures for becoming accredited, handling complaints and dealing with any failure or non-compliance of the accreditation schemes. Ideally these would be developed by consensus in consultation with industry and other relevant stakeholders.

APPENDIX K: TCF ENUM Working Party Project Scope

Telecommunications Carriers' Forum Incorporated

Project Scope

Date Submitted: 5 October 2005

A: Background

ENUM is relevant not only to telecommunications carriers and their customers, but to all ICT companies. Previously, Internet NZ commissioned their own internal ENUM report to explore similar issues to those set out below. While the InternetNZ scope of work is somewhat relevant to the TCF members, it does not necessarily address, or give the same priority to those issues which most affect telecommunications carriers and TCF members in particular.

Although some countries now have a live ENUM environment, many of the ENUM trials undertaken overseas have achieved little in relation to defining robust policy and process flow information. These trials have focused more on the evolving technological issues with a specific focus on DNS. From a strictly telecommunications perspective, many of the issues likely to arise as a consequence of, or in relation to ENUM, have not yet been identified let alone addressed.

The TCF Rule (Rule 4.1(c)) allows the TCF to establish working parties for the purpose of "facilitating dialogue on industry issues of common interest and (if agreed) work together to address these issues".

B: Working Party Project Brief

As per clause 7.1.1 of the Forum Handbook, this Project Scope is based on the Project Proposal submitted by Telecom and approved by the TCF Board on 4 May 2005.

The Working Party's project brief is to:

i. Identify and summarise overseas ENUM trials with a particular emphasis on distinguishing the differences between a regulated and non-regulated environment;

ii. Within the context of each ENUM trial (or country) analysed, investigate the potential issues encountered by Telecommunications carriers, their customers, and the associated government agencies.

iii. Consider how ENUM might affect, or be affected by current (and draft) Codes prepared by the TCF; and current projects in implementation, particularly Number Portability

iv. Consider possible transition and interoperability issues relating to the co-existence and potential interconnection between ENUM and traditional telephone numbering regimes;

v. Consider how the introduction of ENUM may affect roaming, existing national and offshore interconnect agreements, and other bilateral arrangements;

vi. Consider the different ENUM options, particularly the requirements for Operator and User ENUM and how these impact on carriers', new entrants,

Internet Service Providers including the implications for eventual use and implementation.

vii. Provide recommendations for the eventual ENUM infrastructure and transaction framework including delegation of .4.6.e164.arpa. This will include possible regulatory requirements, process flows based on differing Registry/Registrar scenarios, policy framework, and potential commercial models for the operation of an ENUM Registry;

viii. Provide recommendations on the Registrar infrastructure. This will exclude the services fabric and will focus on terms of engagement, billing flows (retail & interconnect), lawful intercept and policing, subscriber privacy and security, and associated counter-measures for fraud and ENUM misuse identification;

ix. Identify potential uses and customer models for ENUM;

x. Identify the requirements and objectives for a meaningful ENUM Trial;

xi. Identify possible legal and legislative issues for later consideration;

xii. Recommend a work plan and next steps for the TCF; and

xiii. Provide regular progress reports to the Board via the Monthly Report**.**

Areas considered "out of scope"

There are several areas identified by the Working Party that will not be covered by the Project Scope. These are based more around the "physical delivery" of ENUM, and as such will not be covered until a planned trial is imminent. It must also be noted that although these areas are considered out of scope, these factors will be considered when making decisions and recommendations on areas that are contained within this scope of work.

The areas that will be specifically out of scope are:

i. ENUM network layer architecture
ii. ENUM services layer architecture
iii. ENUM interconnect architecture
iv. Billing architecture – both at a Registrar and ENUM Service Provider level
v. Identifying possible business models and the economic issues raised

The Working Party will also ensure that the work of the Joint ENUM Steering Group is taken into consideration.

Proposed Public Consultation

The Working Party does not consider there is a need for any public consultation during this initial scoping and investigative phase.

C: Legislative Obligations

ENUM at this point in time is not a 'designated' or regulated service, and as such is not directly subject to any legislation. However, all Carriers are still subject to the Telecommunications Act 2001, and as such, any possible impacts of complying with the Act will be considered whilst the Working Party undergoes it's investigations and prepares it's report to the TCF Board. These legislative obligations will also be taken into consideration when planning the viability of a future ENUM trial.

D: Deliverables

The deliverables from this project are:

- A preliminary report as per rule 7.1k of the Forum Rules that recommends whether or not work should continue (given it is a non-regulated service); and

- A final report that identifies ENUM issues for New Zealand telecommunications carriers and their customers, and recommend next steps for the TCF with regard to this issue. It is anticipated that the report would be submitted to the Commerce Commission and the Ministry of Economic Development for their review and feedback.

E: Working Party Membership

i) TCF Members

	Name	Organisation	Email
Project Leader:	Richard Jeffares	WorldxChange Communications	rjeffares@wxc.co.nz
Working Party Members:	Brett Thomson	WorldxChange Communications	bthomson@wxc.co.nz
	Simon Paxton	Callplus	simonp@callplus.co.nz
	Ernie Newman	TUANZ	enewman@tuanz.org.nz
	Mark Corbitt	Telecom	mark.corbitt@telecom.co.nz
	Ritesh Prasad	TelstraClear	ritesh.prasad@team.telstraclear.co.nz

F: Resource Requirements

The following amounts have been allocated to this project in for the 2005 budget:

September 2005	20 hours @ $150 per month	
October 2005:	10 hours @ $150 per month	
November 2005:	10 hours @ $150 per month	
December 2005:	10 hours @ $150 per month	
January 2006:	10 hours @ $150 per month	
February 2006:	20 hours @ $150 per month	
March 2006	20 hours @ $150 per month	
April 2006	20 hours @ $150 per month	
TOTAL BUDGET	**110 Hours @ $150/hr**	**$16,500.00**

The proposed project timeline in the next section indicates the work that the Forum Administrator will be involved with each month (through regular teleconference meetings etc), and the Working Party will endeavour to keep within the budget constraints detailed above.

Budget Reporting

The Working Party requests that the Forum Administrator report to the Project Leader when hours allocated to a particular month are reaching their limit, so that the members can:

- Use internal resources instead; and/or
- Indicate to the TCF Board that more funding may be necessary; and/or
- Direct the Forum Administrator resource to the most useful tasks.

G: Proposed Project Timeline

The table below shows a proposed Project Timeline.

Milestone	**Date**
Board Approval for commencement	July 2005
Preparation of project scope by Working Party	23 September 2005
Board signoff on project scope	5 October 2005
Expected Release Date for Full ENUM Report	1 May 2006