

UK ENUM TRIAL GROUP (UKETG)

STATUS REPORT ON THE TRIAL IMPLEMENTATION OF ENUM IN THE UK

MAY 2004

Issue 1.1

TABLE OF CONTENTS

SYNOPSIS	4
EXECUTIVE SUMMARY	5
1 Glossary of Terms	8
2 Introduction	9
3 Working methods	11
4 Top Level Principles	13
5 The Participants and their roles	17
6 The Top Level Process	20
7 Overview of Interfaces between Players	22
8 Details of Registry Role and Issues	24
9 Detail of Registrar Role and Issues	26
10 Detail of DNS Role and Issues	29
11 Detail of Authentication Role and Issues	34
12 ENUM Security Threat Analysis	44
13 ASPs and Trial Applications	45
14 Accreditation	52
15 Legal Considerations	53
16 Open issues	55
17 Future of UKETG	57
18 History of the Report	58
Annex A – Companies and organisations active in the UK ENUM Trial Group	59
Annex B – Terms of Reference for the UK ENUM Trial Group	60
Annex C – User Memorandum of Understanding	63
Annex D – Administration of the Meta Registry for 4.4.e164.arpa	68
Annex E – Accreditation for UK Production ENUM	69
Annex F - UK ENUM Legal Considerations – Industry	76
Annex G – UK ENUM Legal Considerations - Participants	78
Annex H – Data Templates	84
Annex I – Attacking ENUM Security	96
Annex J – Trial Participants Remarks	100

TABLE OF FIGURES

Figure 1 – Meta Registry and functional roles in the trial	12
Figure 2 – Players in ENUM	17
Figure 3 – Interfaces between players	22
Figure 4 – Tier 1 Registry Interfaces	24
Figure 5 – Registrar Interfaces	27
Figure 6 – DNS Provider Interfaces	32
Figure 7 – Authentication Agency Interfaces	34
Figure 8 – ASP Interfaces	45

This document consists of 1 pages

SYNOPSIS

This report formally places all the UK ENUM trial results into the public domain. The trial, with the full support of the DTI, has laid strong foundations for future ENUM and ENUM dependant activities within the UK and has dealt with all the objectives originally outlined in the Memorandum of Understanding including important issues such as competition. This report shows how best the industry and other interested parties can progress to allow a UK ENUM industry to crystallise, develop and thrive after a period of consultation.

The trial broadly succeeded in testing the architectural, technical, operational, and end-user aspects of provisioning ENUM services for country code +44, and has provided an invaluable wealth of experience, data, and other information relating to the likely implementation of such systems. The trial revealed practical solutions that can be used to move forward into a full commercial stage that would meet the need for an open and competitive market that adequately protects the interests of individuals and enterprises alike.

The UK trial has been at the cutting edge, and shows that ENUM has the potential to unify many different communication standards and mechanisms. ENUM could revolutionise previously diverse technologies and markets over the coming years and may become a very important element in the process of convergence between the traditional telecommunications world and the world of the Internet.

There remains further work to be undertaken in the area of the economic costs and benefits of ENUM and ENUM related services as well as practical implementation of authentication mechanisms. The trial has defined the challenges to be met before ENUM can realise its potential and become a prolific, new enabling technology solution for the 21st Century.

EXECUTIVE SUMMARY

The work undertaken by the UK ENUM Trial Group (UKETG) during the national ENUM trial is described in this report. The trial operated from December 2002 until December 2003. It was carried out by a number of participants from industry and its purpose was to identify the advantages and disadvantages of the approach to ENUM that was suggested by the report produced by the UK ENUM Group (UKEG) in 2002. Experience gained in the trial would inform UKEG about various technical and policy matters concerning the deployment of an ENUM system for the UK.

In general terms, the trial was successful. However there were some disappointments and a number of issues remain to be resolved. These are described in the report. Substantial progress was made in the areas of authentication and accreditation. This work will lay the foundations for a successful and competitive ENUM system. UKETG has produced detailed documentation on the interfaces and processes between the various entities that will be involved in an ENUM system. The roles and responsibilities of these entities have been identified. These are the main successes of UKETG's work. Sections 5-13 of the report describe the work on these topics in detail.

The work of UKETG has provided valuable practical guidance on how to provide the infrastructure and operating framework for a production ENUM system. It has also helped to identify the roles, responsibilities, procedures and processes for ENUM. These are very significant achievements.

UKETG did an enormous amount of work on authentication and validation. This is a very hard problem. There are a large number of awkward corner cases (for example, DDI blocks, pay-as-you-go mobile phones, premium rate and non-geographic numbers, and so on) that present difficult challenges. Other obvious challenging cases include ex-directory numbers and households when many people share the one phone number. UKETG has demonstrated how to perform authentication with or without the participation of the relevant telephone company. This is a very valuable result from the trial. Even so, more work still needs to be done in this area.

There are two potential solutions to this difficult problem. One would be to consider adopting a lightweight form of authentication, perhaps something as straightforward as a first-come, first-served basis for registrations with a simple but quick appeals mechanism to prevent speculative ENUM registrations. However this lightweight approach has not been considered by UKETG. Consultation with DTI and Ofcom would be required before this approach could be explored further.

Another solution would be to undertake further work in co-operation with a telephone company so that an on-line authentication system could be implemented. However it has so far been difficult in the current financial climate to present a convincing business case to justify the effort that would be required.

Excellent results have been achieved on the issues of accreditation and the Authentication Agencies. UKETG has produced good models of how these should operate. These should be acceptable to industry and other stakeholders such as Ofcom

and OFT who will be concerned that ENUM operates under a framework that's fair, open, competitive, and for the public good.

Co-operation between the trial participants was very good. However there were the occasional communication difficulties caused by having a high number of participants based in different locations. Conference calls and mailing lists helped to contain these problems. Deadlines for deliverables were sometimes delayed because of other work pressures on UKETG members. This was a regrettable, but inevitable, consequence from the voluntary way in which the work of the trial was carried out.

There were some disappointments in the trial. One of the main setbacks was in the initial project plan. It was originally expected to have the work of UKETG completed within six months. That turned out to be a too optimistic target given the amount of work that UKETG set out to do. As work on the trial progressed, it quickly became clear that more time would be needed. In retrospect the original scope and time-line for the trial was too ambitious. The trial was extended for a further 6 months. Even then a number of issues remain unresolved. These are described in Section 16.

There was limited opportunity for interaction with other national trials. Some of these had limited scope. Others were slow to make progress or had a different focus. This meant that throughout the trial UKETG has been at the bleeding edge of ENUM development and has almost always been breaking new ground. Some UKETG members were able to exploit those experiences and lessons for their participation in other trials.

Operating the trial with three Tier 1 providers was unsatisfactory. It introduced additional complexity and created operational problems that might otherwise have been avoided. For instance three sets of name servers, one per provider, needed to be checked rather than a single set under one administrative control. Registrars needed to know and keep track of which parts of the UK number space were allocated to which registry operator. The UKEG report recommended a single Tier 1 Registry and the experience during the trial confirms this approach should be the one to follow.

A small number of registrations were processed during the trial, which meant experience with end users and applications has been limited. This was mainly caused by the low visibility of ENUM-based applications and services for users to try. That meant there were few incentives for registering numbers in the trial's ENUM system. A further contributing factor was that UKETG did not have an outreach programme to attract users or other trial participants. A catch-22 situation emerged. Few people registered because there were few applications or services to try. ENUM-capable services and applications were slow to emerge because the low number of registrations suggested demand would be low. Breaking this deadlock proved to be difficult.

Although more ENUM-based applications emerged towards the end of the trial, it is fair to say that, at the time of writing, the "killer application" for ENUM has yet to appear. Even so there are very encouraging signs that Voice over IP (VoIP) and Session Initiation Protocol (SIP) solutions could by themselves make a compelling case for huge numbers of ENUM registrations. ENUM applications are available and their numbers are growing. It is just a question of time before the killer application emerges that will make ENUM as pervasive as the world wide web and email addresses are today.

UKETG identified a number of open issues that require further study. These include financial modelling and an assessment of how transactions will be processed. No on-line authentication system was built. This could be essential for a production ENUM system so that the costs of registration are low and also to ensure large numbers of registrations can be processed efficiently.

During the trial UKETG found that some topics were out of scope for the trial. The most significant of these was the need for an organisation to oversee a national ENUM system. UKETG has recommended that some form of self-regulating ENUM Policy Group should be formed. This would have representation from all stakeholders and be responsible for policy matters such as accreditation, a disputes and complaints procedure, and scrutiny of the Tier 1 Registry.

Although the formation and structure of this Policy Group is beyond the scope of this report, these matters are a serious concern for the members of UKETG. Work on the trial has been self-funding. Members covered their own costs and overheads that were mainly allocating staff to spend time on trial activities. The formation of this Policy Group will incur real costs for consultancy fees, legal expenses and so on. It will be difficult in the current financial climate to make the business case for industry financing this activity. An even harder problem will be making that case when it is not clear how this Policy Group would be constituted or what the return on investment would be, assuming there even was any. It may be that this has to be an area where support from government and Oftel will be crucial. Public money provided for pump-priming the UK's ENUM system could perhaps be recovered at a later date: for instance by some form of revenue sharing from the Tier-1 registry operator for a commercial ENUM service or through accreditation/licensing fees. UKETG recommends that UKEG discusses these matters with DTI and Oftel.

1 Glossary of Terms

DTI	Dept of Trade and Industry
UKEG	UK ENUM Group
UKETG	UK ENUM Trial Group
UKEPG	UK ENUM Policy Group
IETF	Internet Engineering Task Force
RFC	Request for Comment
ITU-T	International Telecommunications Union – Telecommunications Standardisation Sector
ETSI	European Telecommunications Standards Institute
Oftel	Office of Telecommunications
Ofcom	Office of Communications (subsumed Oftel at end of 2003)
OFT	Office of Fair Trading
DDI	Direct Dial In (block of individually addressable numbers connected via a single network interface)
PSTN	Public Switched Telephone Network
NP	Number Portability
DQ	Directory Enquiries Service (from Database Query)
TSP	Telephony Service Provider
IP	Internet Protocol
DNS	Domain Name Server
RR	Resource Record (data record stored and returned from DNS)
NAPTR	Naming Authority PoinTeR record (a kind of RR used in ENUM)
URI	Uniform Resource Identifier
VoIP	Voice Over IP (Voice samples carried in IP packets)
SIP	Session Initiation Protocol (A VoIP signalling protocol)
DNSSEC	DNS Security Extensions (Secure DNS)
TSIG	Transaction Signatures (used with Secure DNS)
IPv6	IP Version 6
RIPE NCC	Reseaux IP Europeens Network Co-ordination Centre
ISP	Internet Service Provider
ASP	Application Service Provider (note – not provider of network access)
AA	Authentication Agency
LDAP	Lightweight Directory Access Protocol
PKI	Public Key Infrastructure

2 Introduction

Following an industry seminar held by the DTI in September 2002, a decision was taken to set up an ENUM Trial Group (UK ENUM Trial Group - UKETG) with the aim of testing some implementation aspects of ENUM in the UK. UKETG was asked to evaluate the ENUM architecture suggested in the UKEG Preliminary Report on the Implementation of ENUM in the UK, and to identify the advantages and disadvantages of that approach for a commercial ENUM system in the UK. This document forms the report of the UKETG.

2.1 What Is ENUM?

ENUM is a protocol defined in RFC3761 that allows the mapping of E.164 telephone numbers into domain names. When those domain names are looked up in the DNS, attributes known as NAPTR records can be returned. Each NAPTR record describes a Universal Resource Identifier (URI). These URIs can identify a number of ways of contacting the owner of the telephone number that was turned into a domain name: phone, fax, email address, web home page, voicemail, PGP keys for secure email, SIP gateway for Internet telephony, mobile phone and so on. In addition each NAPTR record has ordering and preference values for the URI associated with it. Note that RFC3761 supersedes the original ENUM specifications in RFC2916 and RFC2916bis.

ENUM is therefore an enabler for emerging telecommunications services and technologies. E.164 telephone numbers can become the unique identifier to locate all the possible ways of contacting a user. The telephone number will become the key for access to all the available communication applications and services. Applications such as Voice over IP using the Session Initiation Protocol (SIP) and integrated messaging services will be able to exploit ENUM. It will also be possible to use ENUM in the set-up and routing of telephone calls. Therefore ENUM will be at the core of the convergence between the worlds of telephony and the Internet.

2.2 Trial Goals

The aim of the ENUM Trial is to test architectural, technical, operational and user experience aspects related to the provision of ENUM capabilities, as defined in RFC3761, for Country Code 44.

Results collected in the trial will enable UKEG, and any other interested party, to gain information and experience on how to provide and implement ENUM capabilities in the commercial phase.

The objectives of the trial as set by the UK ENUM Group were:

- To evaluate the pros and cons of the different options developed by UKEG to implement ENUM capabilities with particular emphasis on the Registry and Registrar role
- To evaluate processes/interfaces/protocols for the interactions between the different parties (Tier 1 Registry, ENUM Domain Name System (DNS) Provider, ENUM Registrar, Application Service Provider, Number Assignment Entity, Telephone Service Provider)
- To determine technical and operational requirements to provisioning ENUM records at Tier 1 Registry and ENUM DNS Provider level
- To assess DNS requirements/ implications in the provision of ENUM services

- To determine security and verification requirements for provisioning and operation of ENUM capabilities
- To test from a technical and user perspective applications based on the use of ENUM capabilities
- To evaluate and refine the economic benefits and costs of supporting ENUM.

The results of the trial will be used by UKEG to determine the preferred implementation framework for the provision of ENUM capabilities behind Country Code +44.

3 Working methods

The UK ENUM Trial Group, UKETG, was formed at the end of 2002 following a workshop hosted by the DTI. Members of UKETG were drawn from the UK ENUM Group, UKEG, and from a number of organisations that expressed interest in participating in a trial. Some companies joined UKETG and took part in the trial once it was under way.

UKEG is the parent body of UKETG, overseeing its activities and getting status reports on the trial as it progressed. UKEG tasked UKETG to examine the practical issues that were identified in the UKEG Preliminary Report on the Implementation of ENUM in the UK. Any problems or policy questions arising during the trial would be reported to UKEG. The separation between the two bodies meant there was a clear understanding of the responsibilities of each. UKETG concentrated on technical implementation issues while the focus at UKEG was on policy matters such as governance models and regulatory considerations.

A Memorandum of Understanding was prepared by UKEG that all UKETG members were required to sign. Legal issues raised by some UKETG members meant the MoU needed to be extended by a supplement. UKETG members elected a Chair and Co-chair. Terms of Reference (See Annex B) for the operation of UKETG and its interaction with UKEG were agreed.

At its initial meeting, UKETG worked out a project plan for the trial. This defined objectives, set deadlines and established dependencies between these. It was felt that the work could be accomplished in 6 months. In retrospect, this target proved to be over-ambitious and the project had to be extended for a further six months. This extension was agreed by UKETG and UKEG.

The work of UKETG was broken down into specific components of an ENUM system: Registry issues, authentication & validation, DNS providers, Registrar considerations and so on. Members of the trial group chose to work on each of these components. A collaborative approach was taken to the work of UKETG. Members agreed to work on the basis of consensus: lack of sustained reasonable objection. This proved to be successful. Although some contentious points emerged during the trial, these were resolved to everyone's satisfaction.

Much of the communication and co-ordination of UKETG's activities was done electronically. Mailing lists were used to exchange ideas and draft documents. There were frequent conference calls. Sometimes these were for the whole group though they were also arranged for subgroups that were working in a particular area. Physical meetings for the whole group were held approximately every 2 months.

3.1 The delegation of +44

Selection of the Tier 1 Registry for the trial proved awkward. Three companies wished to take on this role. For a number of reasons, it was not possible or practical for this to be operated by single, shared entity or to have the role rotated between the three candidates. A pragmatic solution was adopted. A meta-registry was set up and operated by the UKETG Chair who had obtained the delegation for *4.4.e164.arpa* on behalf of the DTI. An analysis was made of the UK's telephone numbering allocation. From this, the UK's E.164 number space was divided into three broadly equally sized chunks. Lots were drawn to delegate each chunk to the three Tier 1 candidates. Although this was a

fair solution, it created additional work and complexity. For example, a Registrar needed to know which Registry to contact for an ENUM registration. This did not materially affect the work of UKETG. Although this arrangement was adequate for the duration of a trial, it would not be satisfactory or suitable for a production ENUM system.

Special care was taken over telephone numbers for the Isle of Man and the Channel Islands. Although these territories are not part of the UK, they have been allocated area codes under the UK's telephone numbering plan. UKETG decided to block registrations of these numbers until the views of the regulators in these territories was established. UKEG, the parent body of UKETG, was given responsibility for contacting the Telecommunications authorities in the Channel Islands and Isle of Man.

The diagram below indicates the architecture of the UK Trial. It shows that business entities can operate in one or more roles. The criteria for the operation of the meta-registry are included in Annex D.

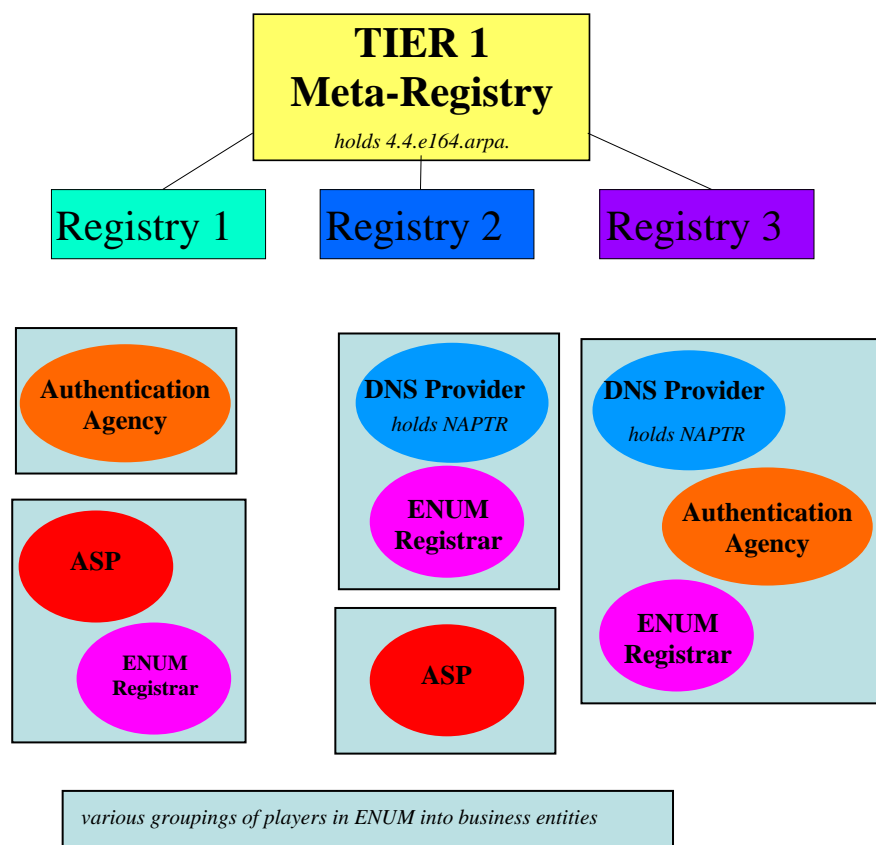


Figure 1 – Meta Registry and functional roles in the trial

4 Top Level Principles

There are a number of top level principles that have proved important as a result of the discussions. UKETG believes that these are general issues rather than artefacts of the particular trial implementations.

4.1 Trust

In order for a customer to register a number in ENUM the all players involved must be reasonably sure that the Registrant has the right to register that number and there must be a degree of certainty that the Registrant is who they say they are. The process to ensure this trust is an integral part of the ENUM registration system is known as Validation and Identification (V&I). The V&I parts of the registration process are known collectively as the Authentication Process.

This requirement ensures that only the authorised telephone number assignee subscribes to, changes, or cancels their ENUM registration and prevents ENUM registration hijacking¹. The validation function shall occur both upon initial subscription as well as on an ongoing basis.

Of course, once a registration is in place, the published data represents a Registrant's contact details; there is a measure of trust that these are correct. Thus it is important that this data is populated, modified or removed only at the behest of the Registrant. Authentication of requests for addition, modification or removal of contact data sent to a DNS Service Provider will also need to be carried out; if not then it would be possible for an attacker to hijack the Registrant's ENUM data. Without authentication of requests sent to the Registrant's DNS Service Provider, all the good work of ensuring that the registration was correctly provided is wasted.

The issue of trust is a particular concern for both the TSP customer and the TSP itself: the TSP customer is concerned that their number not misused within the ENUM system leading to the possibility of communications to them being misdirected or personal distress. Their TSP is concerned that the number is not misused, as this might reflect on their general competence and cause a loss of revenue in their ENUM-unrelated business.

ENUM registration and data hijacking can be regarded as the most serious risks to ENUM if the registration process is not implemented in an acceptable manner.

4.2 Equal Access

In order for ENUM to be a commercial success it must be ensured there are no artificial barriers to registration in terms of cost, time-scale or restrictive business practices. There must be equal access for all prospective ENUM Registrants to enter any valid UK telephone number irrespective of a TSP's awareness of ENUM.

This causes a problem for the ENUM registration system in that, although a TSP authentication system is probably the most robust system available, not all TSPs will be willing to be involved in this process.

¹ ENUM registration hijacking is defined as the provisioning of an E.164 telephone number into any ENUM DNS Registry by an unauthorised entity, i.e. by someone other than the assignee of the E.164 telephone number.

This brought forward the concept of a Participating TSP (PTSP), which can be defined as a carrier who is willing to participate in the V&I part of the registration process for their users in a non-restrictive manner. Also, there is recognition that not all TSPs will be able or willing to participate so there must also be a secondary process allowing customers of a non-participating TSP to complete the ENUM registration process.

It was agreed by the UKETG that if a TSP participates then the recommended process should be to channel authentication requests through the participating TSP to ensure a robust (trusted) authentication.

Authentication of numbers belonging to a non-participating TSP will be dealt with through a secondary (basic) process that is defined in section 11.

4.3 Value

In order for ENUM to succeed, costs must be set at a reasonable and bearable level to the end user.

Given the UKETG agreement that the recommended process should be to channel authentication requests through the participating TSP, there is some concern that this monopolistic position may lead to the TSP electing to set unreasonable charges in order to restrict the uptake of the service.

Therefore, if a TSP decides to participate in the trusted authentication process, they should provide authentication data and service at a reasonable cost in order to allow the ENUM Registrant successfully to authenticate the number. It will be responsibility of the group appointed to oversee the ongoing implementation of ENUM in the UK to monitor and ensure TSPs, and any other source of trusted data required for validation and identification, provide their services and data at a reasonable costs and do not act in a way that may negatively affect the services offered by the Authentication Agency.

The authentication process should be designed to be as automated as possible to reduce processing costs.

4.4 Regulation

There is a general consensus that ENUM should not require regulation in the way that the telephone system is regulated. A strict regulatory regime is likely to hinder the deployment of ENUM and the provision of new services or applications based on this technology. However this should not mean that ENUM would operate in a policy vacuum. Some form of oversight will be needed. Ideally this would be achieved through a self-regulating framework with participation from stakeholders. This body could deal with disputes, accreditation issues and so on. It is expected that this body may be analogous to the way ICTSIS oversees the operation of premium-rate telephone services. For the purposes of this report, this oversight body is called the UK ENUM Policy Group (UKEPG). A decision about the name of this body, its composition and remit is not for UKETG. It is assumed this will be determined by UKEG in consultation with DTI and Ofcom.

4.5 Free Market

A principle of a free market operates within ENUM and as a result it is understood that, although desirable, TSPs are not compelled to participate.

Various business entities can perform multiple roles at Tier 2 and in some cases a bundled service may be provided. This principle is illustrated in diagram 2. Shown are different cases in which Registrars, Authentication Agencies (AAs) and DNS Providers may provide one or more functions.

4.6 Responsibility

Each entity in the ENUM system has a responsibility to ensure that the systems and processes put into place are as fair and secure as possible.

It is not clear who or what entity has an overall responsibility for representing consumers' rights with respect to protection and privacy issues. It is understood that the ENUM system will be organised to best protect customers. However, more thought should be given to this area before commercial launch. One suggestion is that responsibility and representation of customers with telephone numbers is ultimately part of the Ofcom role as it is the Number Administrator for the UK and therefore may also require the Ofcom's Consumer Panel involvement.

The Trial Group did, however, reach consensus that it is the responsibility of the Registrant to inform the Registrar and/or any other relevant parties in the ENUM system if an event occurs that would change the nature of the ENUM subscription, for example: termination of telephone service associated with the ENUM domain or porting of the telephone service to another provider.

In other words players in the ENUM registration process (especially the Registrar and AA) will NOT take a pro-active role in ensuring that the ENUM registration is constantly valid. After the initial identification and validation, it is assumed that ENUM registrations will remain valid until they are due for renewal, unless the Registrar is otherwise informed by the Registrant.

4.7 Duty of Care

The potential for misuse means that the entities in an ENUM system will have a duty of care on the management of the data they store and, in some cases, publish. These could include contact details, authentication credentials, billing information and so on.

Safeguards will be required to minimise the risk of fraudulent registrations or unauthorised manipulation of a user's ENUM data; these particular problems are known as number hijacking and data hijacking respectively.

Some of these concerns will be addressed either by existing legislation on data protection and privacy or by Ofcom regulation. Others could be handled by the framework for codes of practice and accreditation suggested in this report. For example, the proposed UK ENUM Policy Group could oversee any accreditation system and provide mechanisms for handling complaints and disputes.

Where hijacking has occurred, the first point of recourse is to the fraudulent Registrant or attacker. However there may be a level of liability accepted by the Registrar and Authentication Agency as part of the V&I process, and potentially by the DNS Service Provider who publishes the Registrant's data (and may have a duty of care to ensure that any request for publication comes from the Registrant).

Further legal and regulatory advice is required on this issue. The current view of UKETG is expressed in section 15 and Annexes F and G.

4.8 Fairness

Service Providers are in a powerful position relative to potential customers, particularly in the early phases of provision of a new service area. To counterbalance this and to stimulate competition, as a general principle a customer should be free to choose the organisation from which they are provided service. A service provider should not be able to block a customer from using a service feature provided by another, or to transfer to another provider for the service they currently offer. Thus, although a particular organisation may provide a set of ENUM-related services, a customer may choose to be provided each of those services from a different supplier, where this is technically feasible.

One aspect of this lies in control of an ENUM registration; it is the customer's registration, not that of any service provider. The essential qualifier for ENUM is that a customer is provided a communications service via a telephone number (or number range). A customer should be able to retain their ENUM registration as long as they are provided with a communications service, regardless of the organisation that may be providing it.

5 The Participants and their roles

This section provides a brief overview of the roles within the ENUM Trial. A more detailed description of the roles follows in the main body of the report and a précis of the active companies can be found in Annex A.

The Registrar, the ENUM DNS provider and the Tier 1 Registry are all involved in registering an ENUM in the DNS. Very much like today when a Domain name is registered e.g. *example.com*, a Registrar and a set of name servers (Tier 1 and DNS provider) are involved in registering and holding the mapping of a name to an IP address.

Where ENUM differs from registering a domain name today is in the fact that the number (which is acting as a name) needs to be authenticated to ensure that a user has the right to register and use that number. This is where the Authentication Agency is involved.

The application service provider(s) can then use the ENUM as the key to accessing other service addresses and so provide applications to end users.

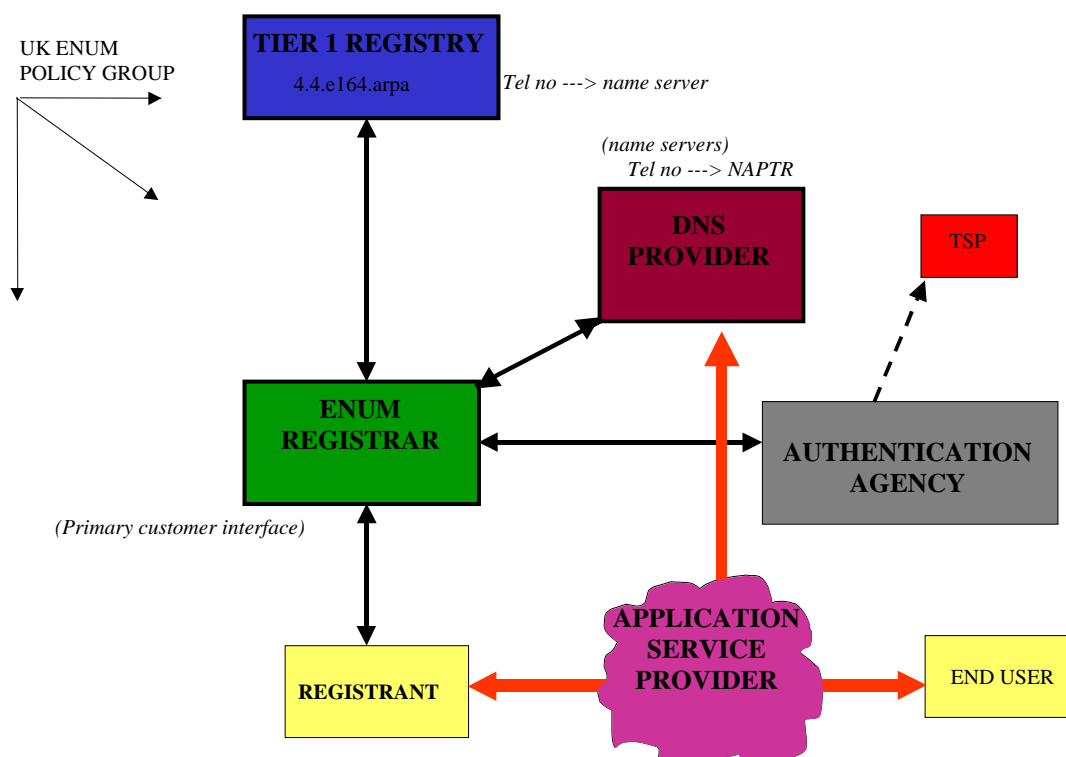


Figure 2 – Players in ENUM

5.1 Tier 1 Registry

The Registry will provide the ENUM delegation, which is required in order to activate an ENUM record. The Registry must be confident that the registration process has been satisfactorily followed prior to enabling the delegation. The confidence in a valid

registration process may be achieved in a number of ways including accreditation of participating entities and/or checking and sending of security tokens.

5.2 Tier 2 Registrars

The Registrar collects all information relevant to the registration of the ENUM and organises the registration. The Registrar may collect a payment from the end user before attempting to validate the registration. If it does so then any information it collects could be used by the Authentication Agency in identifying the user (i.e. it may fulfil the criteria of identifying the person as part of the Authentication function).

5.3 Authentication Agency

The Authentication agency is ultimately responsible for the identification and validation of the Registrant. Given that an AA may choose the market in which they operate, the AA may choose to authenticate: only Directory Enquiries (DQ) numbers; certain TSP numbers, i.e. numbers of TSPs to which they are affiliated, or any one of a number of combinations. In the situation where an AA is using a TSP as the prime data source for Authentication then they will function as an interface between the Registrar and the TSP. If the AA is not implementing their own user identification process then they must initially ensure that the Registrar has used due care in identifying the user before attempting to validate the user's right to use the telephone number.

All AAs will be permitted to choose which Registrars to work with and set their own commercial terms as required. However it should be the role of the UK ENUM Policy Group to encourage at least one AA participating in the commercial phase to cover each type of authentication such that Registrants are able to take advantage of ENUM irrespective of their TSP.

5.4 DNS Provider

This role is responsible for providing an infrastructure of name servers to provide DNS service for the end-user's ENUM zone or zones. Their name servers should be operated according to the criteria defined in section 10.4. Access controls may be necessary to authenticate and manage fine-grained control over which applications and applications service providers are allowed to manipulate the end user's NAPTR records.

5.5 Application Service Provider

Application Service Provider(s) (ASP(s)) are entities that provide end user functionality based on the ENUM platform and data inserted within the ENUM zone file. This can include simple everyday Internet service addresses such as a static email address or Web page location, conventional telephony services such as a switchboard number or fax machine or "next generation" services such as VoIP, LDAP directory services or PKI keys that may need to modify the DNS records for the ENUM zone in real time. ASPs may act as a reseller of Registrar services that are provided by third parties or may be the users' incumbent ISP or TSP. There are, and should be, no restrictions where entities act purely in this Role.

5.6 TSP

It is agreed that TSP participation is the preferred mechanism of ENUM authentication as it provides the maximum level of trust in the registration, as such once a TSP is participating it will make a suitable interface available to all accredited AAs.

AAs will be compelled to use this interface in order to ensure the registrations are trusted; however due to this restriction a number of safeguards must be put in place with regard to the TSP interface to avoid the potential of abuse.

A process is required in order to classify a TSP as participating, the goal of which is to ensure the TSP's users are authenticated using the most trusted method whilst permitting and encouraging competition within the AA marketplace. At any time a TSP may choose to run its own AA and or Registrar in order to service their own customer base or others.

5.7 UK ENUM Policy Group (UKEPG)

It is suggested that a self-regulating body would be formed to oversee the operation of an ENUM system in the UK. This body would have representation from the key stakeholders: the participant roles outlined in this report, government, Ofcom and so on. It would formulate the rules and policies underpinning the implementation of ENUM; providing the checks and balances to ensure fairness, transparency and equality. This proposed body could oversee any accreditation systems and likely codes of practice that may be required for any of the roles in an ENUM system: Registry, Registrar, and so on.

The UKETG assumes that such a body will be created and recommends that the UKEG considers the formation of this body. The structure and remit of this UK ENUM Policy Group is outside the scope of UKETG. For the purposes of this report it is assumed that a body will be created that broadly has these responsibilities and this body is known as the UK ENUM Policy Group (UKEPG).

6 The Top Level Process

An overview of the registration procedures and the interactions at each stage of the process are described in the following section. More detailed descriptions of the interfaces are provided in subsequent sections.

6.1 Information Collection

The Registrant requests the Registrar to register a new ENUM domain name. The Registrant can choose the preferred Registrar among the recognised ENUM Registrars. Registrars should provide a suitable user-friendly interface to allow simple and easy interactions with the Registrant. During this phase the Registrar will collect information to be passed to the AA in order to validate the user such as the name of the user's TSP, any relevant customer numbers and or supporting information and also the details of the DNS provider the Registrant wishes to use.

6.2 Validation Information Collection

The AA should provide a secure interface to the end user via the Registrar where needed to permit the collection of information that may be commercially sensitive such as TSP account number. This interface may be realised between the TSP and the end user, but the AA will be responsible for ensuring that the information can be collected securely.

6.3 Identification (Preliminary)

The Registrar attempts to Identify the user, preferably using an automated process such as making a charge to a credit or debit card registered by the user at the Telephone number service address. Where this is not possible supporting documentation may be required. Suitable procedures would form part of the Registrar Code of Practice to be drawn up by the Registry and UKEPG.

6.4 Authentication (Identification & Validation)

The Registrar requests that the AA authenticate the registration attempt by forwarding all relevant information. On receipt of this the AA concerned may review the Identification information forwarded to confirm the user's identity and ensure compliance with the code of practice, or may implement its own identification procedure. The AA then validates the request via either a participating TSP or the secondary process if appropriate (see later). If successful, the AA informs the Registrar they may continue with the registration and passes an authentication token. The AA may request additional supporting information from the Registrar at any time.

6.5 Zone Creation

The Registrar notifies the chosen DNS provider to create a zone file associated to the new ENUM domain name. The DNS provider should provide a user-friendly interface to allow simple and easy interactions with the Registrant. The interface may differ from DNS Provider to DNS Provider. Note in many situations Registrars are likely to also offer DNS services.

6.6 Registry Submission

The Registrar passes all the required information for the registration and zone delegation to the Registry including the relevant AA authentication token (Annex H describes in more detail the interfaces and interactions between Registrar and Registry). This will be done by passing a form of secure token defined between the Registry and AA that is outside the scope of this document.

6.7 Registry Insertion

The Tier 1 Registry processes the request, creates the zone delegation and returns a notification of the registration and delegation to the Registrar. If the Tier 1 Registry is not able to process the Registrar's request (i.e. incorrect/incomplete information is detected in the registration form) the Registry will inform the Registrar about the reasons for not completing the ENUM domain name registration.

6.8 Registrant Notification

The Registrar informs the Registrant about the results of the ENUM domain name registration.

6.9 Privacy and Security Considerations

It is clear that a token must be devised to ensure secure communications between the Registrant, Registrar, AA and TSP without revealing sensitive data to those parties that do not explicitly require this. There are a number of technical methods in which to achieve this. However the design of this is dependent on the methods of authentication adopted for a commercial roll-out and as such cannot be defined further at this time.

7 Overview of Interfaces between Players

The diagram below illustrates the interfaces that exist between the players during both the ENUM registration phase and the operational phase (i.e. when ASP(s) use the ENUM data to initiate applications).

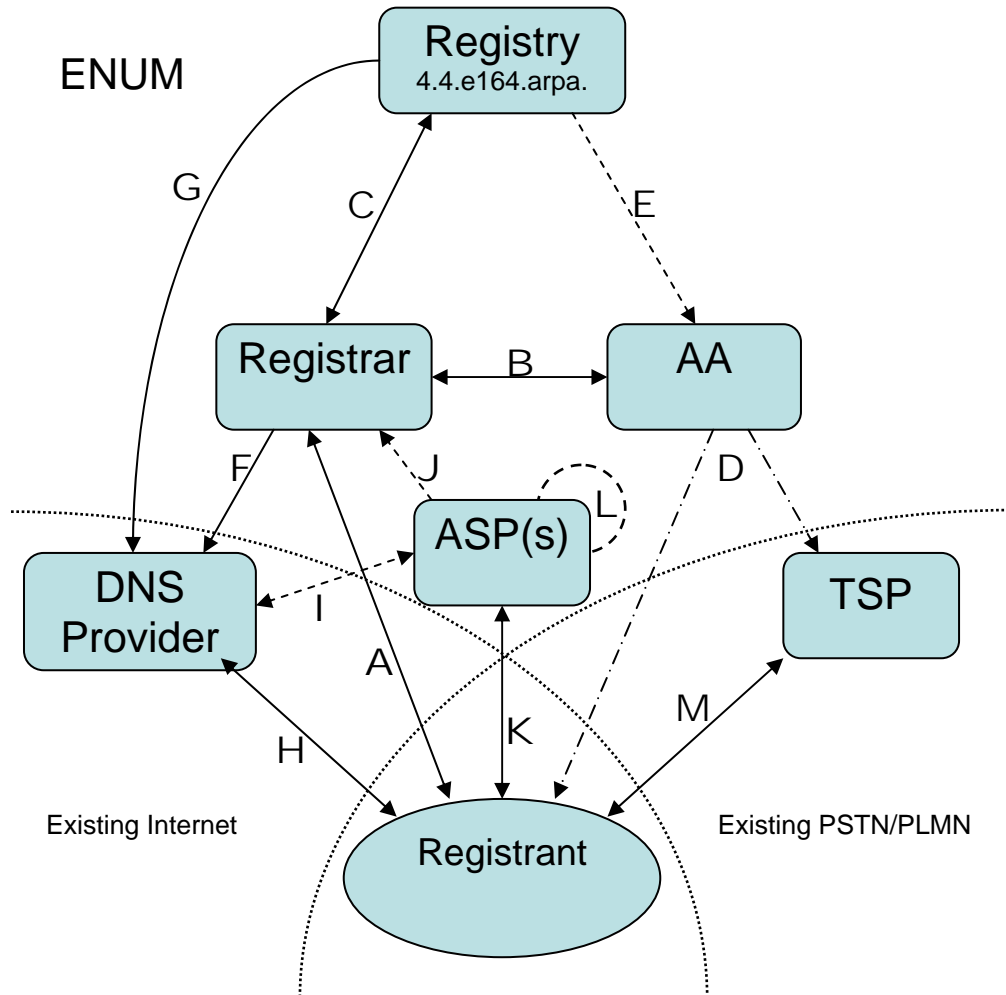


Figure 3 – Interfaces between players

In the following sections each interface is discussed in more detail. However, a summary is given here:

- A: Registrant to Registrar – Mandatory; described in section 9.2
- B: Registrar to AA - Mandatory; described in section 9.2
- C: Registrar to Registry - Mandatory; described in section 9.2
- D: AA to TSP or via DQ/PIN Code - Mandatory - either choice is acceptable; Described in sections 11.2.1.1 and 11.5.3
- E: Registry to AA - Used for checking authentication validity and auditing.
- F: Registrar to DNS Provider - Used to check if DNS servers exist + inform when to set up and remove zone – Mandatory; described in sections 9.2 and 10.6
- G: Registry to DNS Provider - Delegation – Mandatory; described in section 10.6
- H: Registrant to DNS Provider - used for managing zone file – Mandatory; described in section 10.6

- I: ASP to DNS Provider - Optional - May be needed for applications that need to modify DNS; described in section 13.1
- J: ASP to Registrar - Optional - Used when ASP is a reseller; see section 13.1.
- K: Registrant to ASP(s) - Mandatory - Customer must have relationship with service provider for that provider to act as their agent; described in section 13.1
- L: ASP to ASP - Optional - May be required if one ASP manages multiple ENUM services; see section 13.1
- M: Registrant to TSP - Mandatory - Customer must have existing TSP.

8 Details of Registry Role and Issues

Three Registry operators provided Tier 1 service during the trial. This created some problems, though the Registries themselves worked well. The UK telephone number space was divided into three broadly equal sections and allocated to the Registry operators. A meta-registry was provided by the UKETG chairman to delegate sections of *4.4.e164.arpa* to each of the three operators. Although this did not present any problems during the trial, it added unwanted complexity. Four sets of name servers had to be set up, managed and monitored: one for each Registry operator and one for the meta-registry. Another complication was that Registrars needed to do more work when processing registrations, as they had to determine to which of the three Registries to send each request. This was ameliorated during the trial by one of the Registries maintaining an “email director” account that passed the initial registration request to the appropriate Registry based on the telephone number. This approach would not be appropriate for a commercial ENUM service.

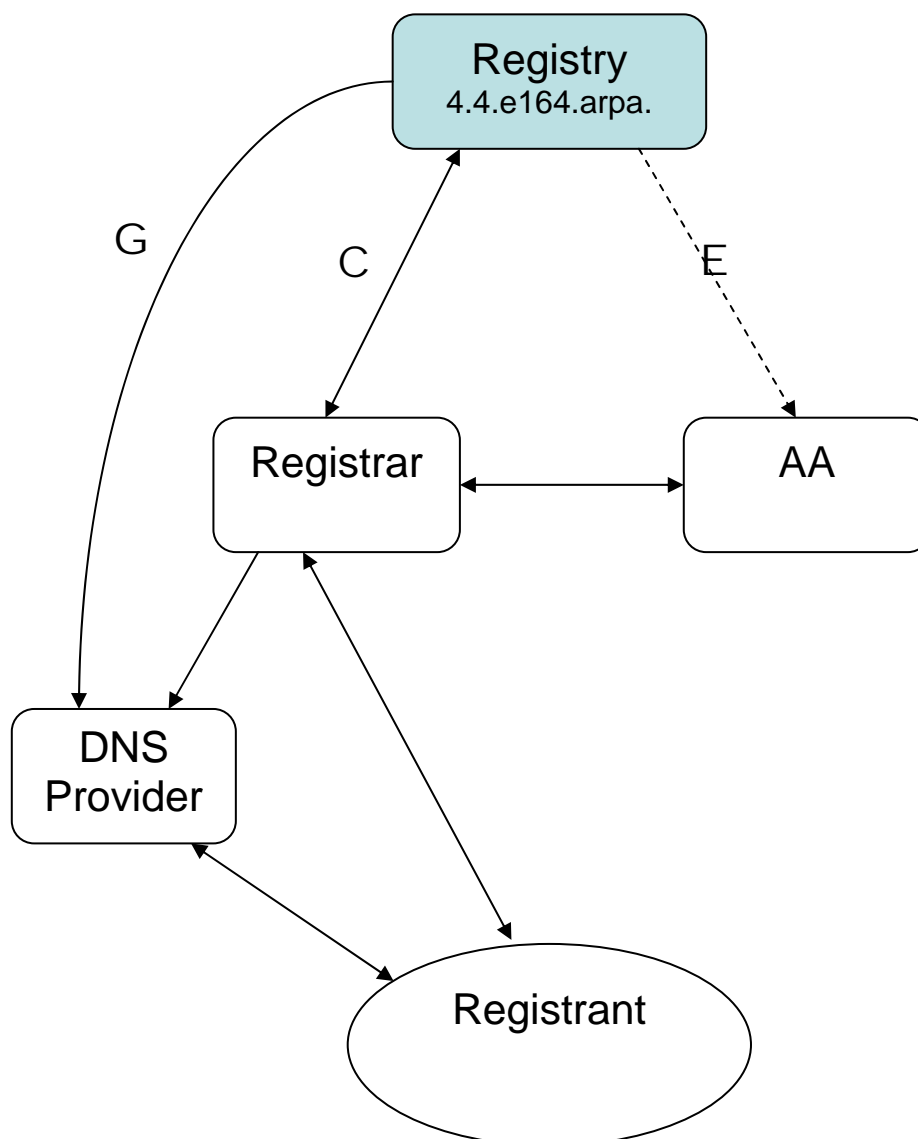


Figure 4 – Tier 1 Registry Interfaces

Initial registrations were handled by email from the Registrars. The interface between Registry and Registrar is described in section 9.2, and the data templates used are described in Annex H.

The interfaces between the Registrar and DNS Provider and Authentication Agency are described in section 10 and 11 respectively.

UKETG discussed the use of the Extensible Provisioning Protocol (EPP) to provide a better interface between Registrars and the three Registries. The outcome of those discussions was inconclusive. An outline template was agreed (See Annex H.3), but only one of the Registries implemented an EPP interface. Time pressures and resource constraints meant none of the Registrars implemented EPP during the trial. This meant the EPP interface was not used, which was disappointing. Further work needs to be done on this topic.

9 Detail of Registrar Role and Issues

The fundamental principles for an ENUM Registrar were defined in the UKEG Preliminary Report on the Implementation of ENUM in the UK. These are shown below. ENUM Registrars will play a key role because they interact with all the other entities that have been identified; the Registry, Authentication Agencies, DNS providers, and the end user. This section discusses these interactions and the typical interfaces that would be used.

9.1 *Criteria and Principles for ENUM Registrars*

The UKEG Preliminary Report on the Implementation of ENUM in the UK (published before the trial, in April 2002) defined a number of criteria that were felt to apply to Registrars. During the trial, UKETG saw no reason to change these criteria; they remain valid, and are given here:

- ENUM Registrars should ideally have prior experience providing Registrar services.
- ENUM Registrars must be able to operate with the interfaces, provisioning systems, and protocols provided by the Tier 1 Registry and Authentication Agencies. They should have flexibility to accommodate changes to those interfaces, protocols or systems should these arise.
- Adequate customer support services should be provided.
- Systems used for ENUM must be operated securely and in accordance with UK privacy and data protection legislation.
- ENUM Registrars must comply with any authentication schemes or agents needed to identify the owner of a telephone number.
- An ENUM Registrar must not use data from an application for any other purposes, including but not limited to entering the telephone number into any other domain, without the express permission of the owner of the telephone number. Similarly, data supplied for any other purpose must not be used to create ENUM entries without that express permission.
- ENUM Registrars must pay the Tier 1 Registry the documented fees in accordance with the terms agreed between them.
- ENUM Registrars must pay the Authentication Agencies the documented fees in accordance with the terms agreed between them.
- Name servers used by an ENUM Registrar to host customer's ENUM data should comply with the DNS hosting recommendations described in section 10.
- ENUM Registrars must provide an audit trail for every registration or attempted registration. This should be made available to the policy group on demand.
- ENUM Registrars must provide an arbitration procedure for Registrants in accordance with the Telecommunications Bill.

9.2 Registrar Interfaces

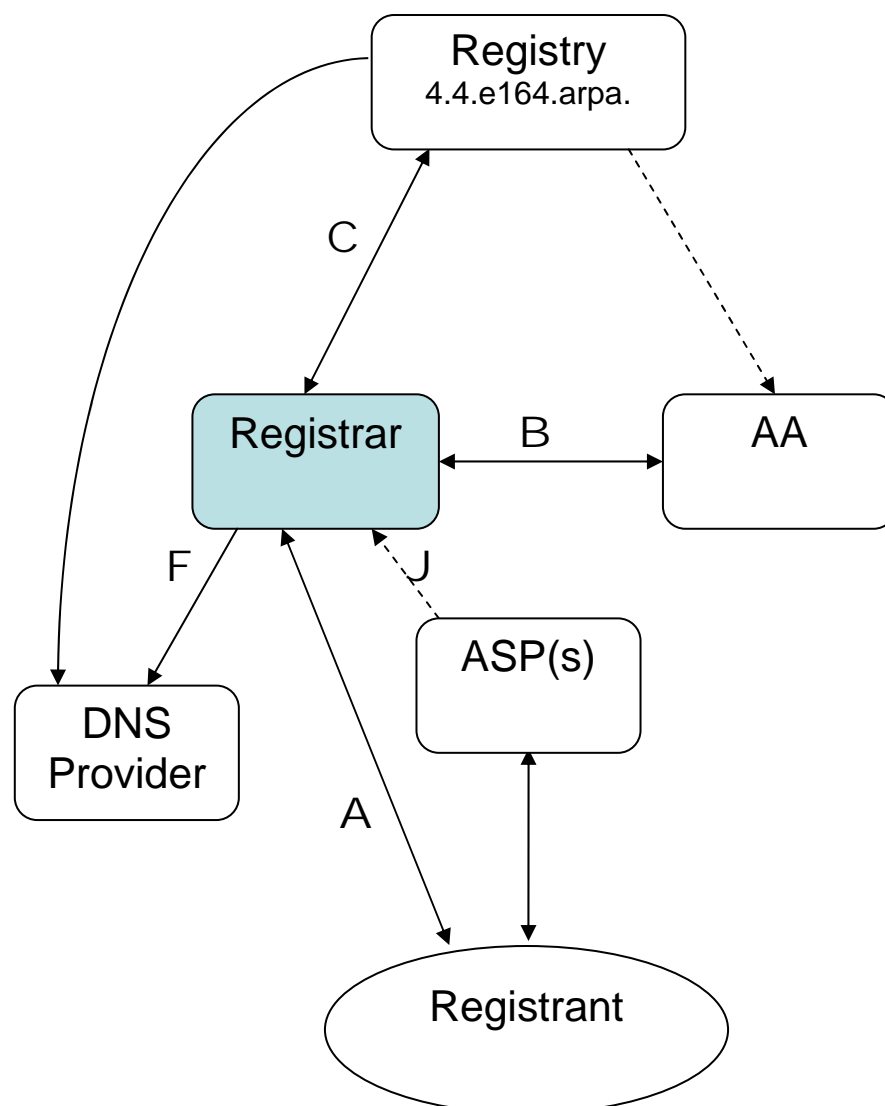


Figure 5 – Registrar Interfaces

The Registrar requires a number of interfaces in order to interoperate with the other entities in the UK ENUM space. As shown above, these interfaces are defined as:

Interface A – Registrant to Registrar

The customer facing interface of the Registrar, this is used to collect information from the aspiring ENUM Registrant as the first step in the process. The information collected by the Registrar is a superset of that required by interfaces B and C with the addition of financial information as needed to facilitate a billing relationship. In a commercial phase this interface should be easy to use, efficient and as self-explanatory as possible.

A working web based implementation of this interface has been built during the trial and is complete excepting collection of financial information.

Interface B – Registrar to AA

This interface uses the information collected in Interface A and comprises the Registrants name and contact details, the telephone number(s) they wish to register and other information used to support the authentication process such as the TSP providing service to this number and/or a PIN Code or other method that may be used to authenticate numbers for a specific TSP or type of e.164 number such as DDI blocks or non-geographic numbers.

Information returned by the AA is expected to show the status of the authentication and contain some form of secure token that can be used by the Registry to confirm the delegation has been authenticated.

The email based interface specification used in the trial is detailed in Annex H.1.

Interface C – Registrar to Registry

Following a successful authentication, or used when modifying an existing ENUM registration, this interface is very similar to those used currently for Domain registration. It contains contact details for the Registrant and also Administrative and Technical contacts and DNS delegation information as well as necessary account handling information such as an identifier and authentication method for the Registrar and the token passed back from the AA in interface B.

The email based interface specification used in the trial is detailed in Annex H.2 whilst an example EPP interface based on this can be found in Annex H.3.

Interface F – Registrar to DNS Provider

Once a successful authentication has taken place, the Registrar must inform the Registrants chosen DNS provider of this fact to enable them to add the zone to their servers. Dependent on the policies defined by a commercial Registry and the UK ENUM Policy Group the Registry may choose to check the name servers chosen for a registration are ready to serve the zone prior to carrying out the delegation, if this was the case this interface would need be bidirectional such that the DNS provider is able to positively confirm readiness prior to the Registrar submitting the delegation to the Registry. This interface is not documented in this report.

Interface J – ASP to Registrar

This interface is included as it is envisaged that during a commercial phase many ASPs will act as a reseller of the Registrar (or Registrars) in order to bundle services to the end user. In this situation the ASP would act to collect the information contained within Interface A. The necessity for the Registrar to collect financial information from the Registrant may be replaced by a billing relationship between the Registrar and ASP. This interface is not documented here, as it would be defined by individual commercial agreements between the Registrar and ASP.

10 Detail of DNS Role and Issues

RFC3761 describes how a telephone number can be mapped into a domain name.

Consider the following example: The requirement is to construct the related DNS domain to look up NAPTR (Name Authority Pointer) resource records associated with the number +44 20 7634 8700 (which corresponds to the main switchboard number at Oftel). The format of NAPTR records is defined in RFC3403.

- Write the E.164 number in its full form, including the country code, then remove all non-digit characters with the exception of the leading “+”
- Example: +442076348700
- Remove all characters with the exception of the digits and put dots (“.”) between each digit.
- Example: 4.4.2.0.7.6.3.4.8.7.0.0
- Reverse the order of the digits and append *e164.arpa.* to the end.
- Example: 0.0.7.8.4.3.6.7.0.2.4.4.*e164.arpa.*

If Oftel had chosen to provision its number in the DNS for ENUM services, the client application could now perform a lookup on this name and, for example, retrieve the NAPTR records for a corresponding fax number, email address or any other URI for the E.164 number +44 20 7634 8700.

10.1 NAPTR Records

The DNS provides a mechanism for storing Resource Records (RRs) for a domain name and a facility for looking up these Resource Records. Clients use the DNS perform lookups to find the addresses of web servers and name servers or to deliver email. With ENUM, DNS lookups will be for domain names like *0.0.7.8.4.3.6.7.0.2.4.4.e164.arpa* and the appropriate name servers would normally return a set of NAPTR RRs.

NAPTRs are simply a particular kind of Resource Record, holding contact details such as a VoIP address, a telephone or fax number, an email address, or a web link. Any client program can send a query to DNS for records of type NAPTR held in the ENUM domain associated with a telephone number, and all the contact details stored in that domain are returned.

The syntax and detailed protocol exchanges are defined in the IETF document RFC3761, with background detail in RFC3401-RFC3404. ETSI has suggestions on how these can be used in trials in their Technical Standard “Minimum requirements for interoperability in European ENUM trials” (TS 102 172).

10.2 Delegation issues

UKETG decided that the Tier 1 Registry would create delegations for each telephone number registered for ENUM. i.e. There would be no delegations at a some intermediate point in the numbering space, for example at area code level. Exceptions were made for the area codes assigned to the Channel Islands and Isle of Man. Technically these territories are not part of the UK, though they have been assigned E.164 numbers out of the UK’s allocation. The regulators in these territories were contacted. At their request

no delegations were made for their area codes during the trial. An understanding will need to be reached with the regulators and other involved parties on how to deploy an ENUM service that will be satisfactory to the UK, the Isle of Man and the Channel Islands. Resolving this issue is outside the scope of the trial.

UKETG analysed the issue of delegating parts of the ENUM name space, typically a block of telephone numbers assigned to a company for DDI. No conclusions were reached and further work is needed in this area. There are advantages and disadvantages to block delegation. The main difficulty with delegating these blocks is that control is transferred from the Tier 1 Registry. This could lead to discrepancies and inconsistencies in the national numbering scheme. The consequences of this are unknown and need to be assessed.

The possibility of number ranges being delegated was also considered by UKETG, for instance by delegating number blocks that have been assigned to a telephone company by Oftel/Ofcom. It was felt this could simplify some authentication issues: the telephone company could easily authenticate the telephone numbers it had assigned to its customers. However number portability considerations make it impossible to assume that all of the numbers in a block are “owned” by one telephone company. There were also concerns that block delegations to telephone companies could enable anti-competitive practices.

10.3 DNS Content Management

Maintenance of DNS zone files is difficult and even DNS experts are known to make mistakes. This problem is exacerbated for ENUM because of the complicated nature of NAPTR records. The format of these records is arcane and very complex. Their semantics are even harder to understand. End users cannot be expected to maintain and manipulate these directly. Tools will be needed. Few tools have emerged so far.

A second problem concerns populating of zone files with resource records. It is expected that applications and tools to add, remove and update NAPTR records will use the DNS Dynamic Update protocol, DDNS, defined in RFC2136. Another approach could be that the tools update a back-end database that then updates the appropriate zone file. In either case, fine-grained control of the updates will probably be necessary. In short, access controls will be needed to ensure an application or tool only changes the resource records that it is permitted to update. Solutions for this are possible. However they are complex to set up and maintain. Once again, end users will need tools. Management of these access controls will be too difficult and involve far too much detail for end users. UKETG has not found any tools for managing DNS access controls yet. These are not expected to emerge until the market for ENUM grows and demand extends beyond the early adopters.

NAPTR records present possible competition issues. Each NAPTR record contains Order and Preference fields. RFC3761 defines how an application processes these fields to choose which NAPTR records to use. Therefore the Order and Preference fields are used to select and prioritise the URIs that an application uses. This flexibility is at the very core of ENUM-based services. However it could be exploited by an unscrupulous application that the user trusts to update their NAPTR records. The application could change the Order and Preference fields of existing NAPTR records to subvert any existing ENUM-based services that depend on those records. For example, Voice over

IP traffic could be diverted to a different SIP gateway from the one that the user expected. No such applications were found during the trial and at present this is felt to be a theoretical rather than a practical problem. Fine-grained access controls will be able to prevent unwanted NAPTR record manipulation, albeit at the cost of more complexity and the provision of better user tools. Even so, it is only a question of time before a zone's NAPTR records get changed in unexpected ways, either by accident or by malicious software.

10.4 Criteria for ENUM DNS Providers

UKETG found that the principles and criteria for DNS Providers that were defined in the UKEG Report on Implementation of ENUM in the UK were satisfactory and do not need to be amended.

However the issue of Secure DNS, DNSSEC, remains unresolved. Protocol specifications have not been completed by the IETF though this is expected soon. Secure DNS will be needed to protect DNS data and verify its integrity. Secure DNS will be crucial for ensuring ENUM DNS data is not exploited for number hi-jacking, spoofing and other undesirable practices.

Further work needs to be done in this area: key management; data signing policies; roles and responsibilities; impact on Registry and Registrar operations, for example. This assumes IETF finalises a standard and implementations of that standard are available.

10.5 WHOIS support

Most DNS Registries are required to operate a WHOIS service to allow the technical and administrative contacts for a domain to be identified. This information should be synchronised with the registration of a domain name, though there is no technical requirement for this. In many cases, the WHOIS information is inaccurate or out of date. An IETF Working Group is developing a protocol that may supersede WHOIS.

In the IETF's ENUM Working Group, no consensus has been reached about providing a WHOIS service for ENUM registrations. UKETG has decided that a WHOIS service was not useful or necessary for the trial. No issues have arisen during the trial so far to contradict that view. UKETG feels there is no technical case to justify the provision of a WHOIS service for a production ENUM service. In fact offering this type of service could cause difficulties with respect to data protection and privacy legislation. However these concerns might be addressed by the new protocol that the IETF's CRISP Working Group is developing.

To date the Trial has not identified any examples of practical technical or operational issues that might have been alleviated by providing a WHOIS service. This does not necessarily mean these problems do not exist or will not arise in the future. However it does suggest that no case has so far been made for the provision of a WHOIS service for ENUM.

WHOIS service can sometimes be useful for conventional domain name registrations, privacy and data mining issues notwithstanding. The service provides a mapping between a domain name and some hopefully truthful and accurate contact information about the owner of that domain name. It might be possible to use that information to

notify the domain owner by fax or phone about a problem with the domain's name servers: email might well not work because the domain's name servers are broken.

For ENUM registrations however, this need for contact information is obviated. The registered domain name provides the essential contact details itself: the domain name owner's telephone number!

10.6 DNS Provider Interfaces

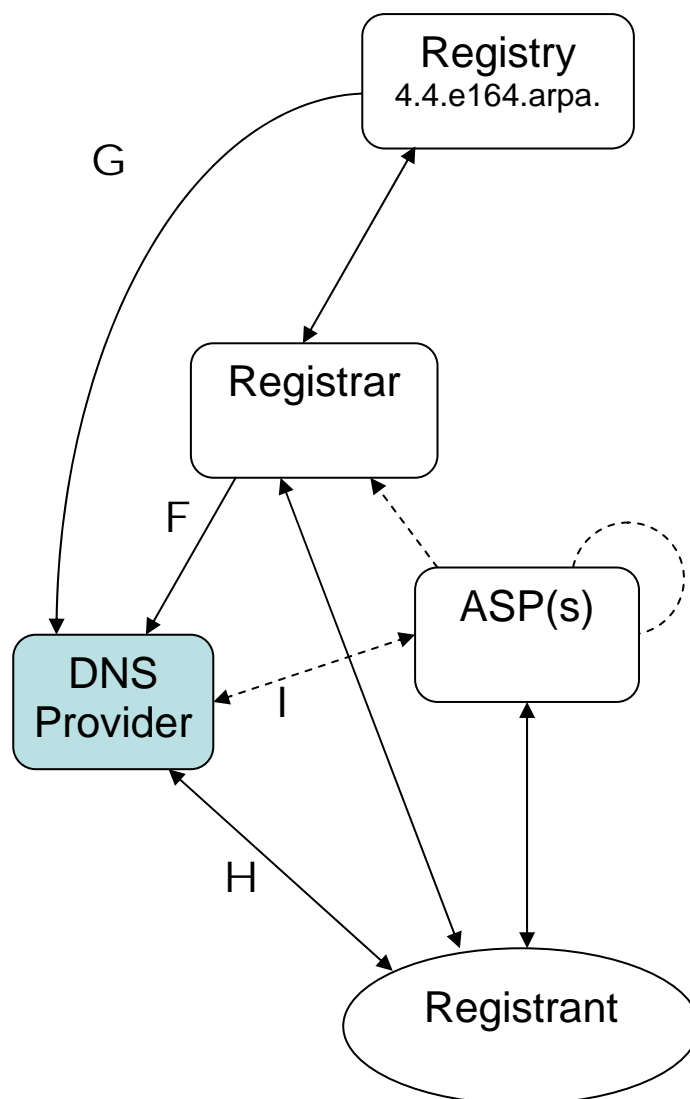


Figure 6 – DNS Provider Interfaces

Interface H – Registrant to DNS Provider

This interface is the standard DNS protocol. H shows the Application Service Provider making a DNS query and the response from some name server. Lookups may also be made to other name servers outside the *e164.arpa* part of the name space. This could happen, for example, when an ENUM lookup returns NAPTR records that identify a SIP gateway or web server in *example.com*. The application or application service provider would need to query the *example.com* name servers to resolve those names.

Interface F – Registrar to DNS Provider

Interface F fulfils a coordination role, and is used only in certain scenarios. First, some Registries require that the Registrar (who is responsible for ensuring that a Registration request is correct) has checked to ensure that the DNS provider is aware of the DNS zone they for which they are to be authoritative, and that the DNS system responds correctly to queries for information on that zone. In another variant, the Registry will allow such publication to be deferred; in this case, the Registrar will inform the DNS provider that the registration has been completed, and they can start to provide responses for the associated zone.

Note that the ASP may be responsible for arranging DNS service on behalf of a Registrant (see section 13 for further details). Reflecting the two scenarios above, in the first case the ASP will have already instructed the DNS provider to start to respond to requests for the zone associated with a potential registration, but the Registrar might still be responsible for checking that the DNS provider was actually doing this. In the second case, an indication that the Registration has been completed would be sent from the Registrar to the ASP, and that entity would be responsible for passing on the indication to the DNS provider.

Interface G – Registry to DNS Provider

Again, this Interface may be required if the Registry decides to communicate directly with the DNS service provider to glean the addressing information for the name servers for a Registrant's zone, or if a DNS service provider needs to communicate directly with the Registry to inform it of a change in the servers that will be used for a registration.

The Tier 1 Registry will provide a delegation to these from *4.4.e164.arpa*. The DNS provider sends the name, IP address and some authentication token to the Registry. If this is validated, the zone's delegation is updated. A successful update will also be reflected in the contents of the Tier 1 zone. The method of transferring this data is will be decided between the Registry and DNS provider and/or the Registrar. Current methods that could be used include text-based email templates, web- or paper-based forms and EPP schemas. These are the usual mechanisms deployed between a DNS Registry and its Registrars.

Interface I – ASP to DNS Provider Interface

This interface is covered in section 13.

11 Detail of Authentication Role and Issues

The various options for authenticating a registration are discussed in this section. At the heart of the many issues that have consumed the time of the UKETG has been Authentication. Authentication is the key difference between registering a normal domain name and registering an ENUM domain. It has the potential to become the biggest barrier to the success of ENUM if all issues are not fully resolved.

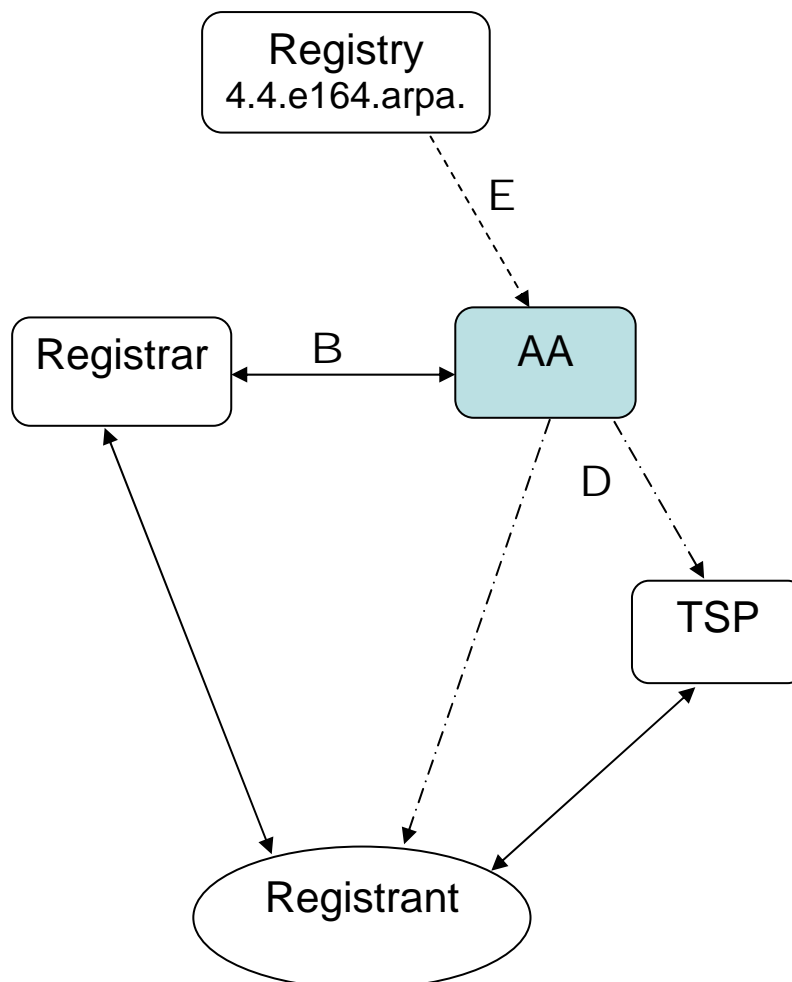


Figure 7 – Authentication Agency Interfaces

11.1 Definitions

Before discussing the principles that have emerged from the discussions it is important to understand what is meant by authentication.

There are two aspects to confirming an applicants right to register a number:

- Confirm that a Registrant has the right to use the number i.e. the name of the Registrant tallies with the telephone number. This function is referred to as Validation.
- Confirm the Registrant is who they say they are. In the following this function is referred to as Identification.

The two processes when combined are referred to as Authentication.

The second item is very difficult to confirm. UKEG agreed that the best that could be achieved would be to tie a name to an address. This would then provide an audit trail.

Thus, the issue of authentication became:

“How to provide proof or evidence that a Registrant’s name can be linked to a particular number and a particular address”?

11.2 Recommended authentication process

The recommended process is a combination of solutions described in the following sections. The process proposed allows for both a ‘basic’ and a ‘trusted’ authentication dependent on level of trust in the process.

The advantage of a ‘trusted’ identification is that it will enable additional services such as digital certificates to be issued for uses such as trusted SIP caller ID. Secure personal identification could perhaps use the ENUM system as a directory for PKI services.

The trusted authentication process must be regarded as the recommended mechanism to ensure that the Registrant has the rights to register a certain number. A direct TSP service, the DQ database and the number portability process have been identified as potential trusted data sources. However, they may not be the only trusted data sources as other industry processes may be used.

When a number can not be authenticated using the trusted authentication method, either because their number is not in the DQ or their TSP is not participating in the UK ENUM industry then a user should still have the right to register a number using a ‘basic’ authentication mechanism. By implication the basic process may use alternate, less rigorous, authentication methods that do not rely on authenticating against TSP data, for example, Caller Line Identification (CLI), and a Personal Identification Number (PIN).

With this understanding, there is no reason to oblige a TSP to participate in ENUM as an Authentication Agency. If a TSP feels they must ensure their customer numbers are adequately protected against misuse then participation in the ENUM authentication process, either directly or indirectly via an appointed agent, would ensure a trusted authentication method is followed for those TSP numbers. If however a TSP is not convinced of the need to participate then their customers are not discriminated against in that they can still register, albeit using a basic authentication method.

It should be noted that if a TSP decides to participate in the trusted authentication process, the TSP has to provide authentication data and service at a reasonable cost in order to allow the ENUM Registrant successfully to authenticate the number without undue or excessive costs. It will be the responsibility of the proposed UK ENUM Policy Group to monitor and ensure TSPs and any other source of trusted data required for validation and identification provide their services and data at a reasonable cost and do not act in a way that may negatively affect the services offered by the Authentication Agency that is ultimately the entity responsible for authentication.

An AA may need to rely on information and data provided by TSPs, Registrars and other sources in order to perform its tasks. It has to offer its services in a competitive, open and transparent way.

In summary:

- If the TSP is participating, then the authentication process **MUST** flow through the TSP (or an agent of the TSP) who will verify a users right to register a certain number. As part of this process it will also be necessary for the TSP to identify the Registrant in order to ensure they are not disclosing verification information to an unauthorised third party.
- If the TSP is not participating then the Authentication Agency will have a number of options, some of which are described in this section, to enable them to authenticate the registration.

11.2.1 TSP Participation Process

As all AAs will be compelled to use an interface once the TSP is classed as participating the issue of approval of commercial and technical terms to ensure they do not put unnecessary barriers to ENUM adoption such as excessive turnaround times, privacy implications or costs needs to be finalised by the UKEG. One possibility would be for this to be a function of any subsequent UK ENUM Policy Group, however this may have an effect on the necessary legal standing of this entity and as such this matter is out of scope of the UKETG and this document.

The Process a TSP should follow in order to be classed as participating will be as follows:

- i) Create and develop an interface to the AAs.
- ii) Set out Commercial Terms for use of this interface.
- iii) Submit interface for external review to ensure it is secure and can be implemented without unnecessary cost.
- iv) Commercial terms should be reviewed to ensure they are reasonable and justified.

If these four stages are completed the TSP will be classed as participating and a “cut off” date when all authentications must use the interface will be agreed. The AAs will then be notified of this new interface and given reasonable notice in order to implement it if they wish to authenticate this provider’s numbers.

The proposed UKEPG should inform all UK TSPs of this process and the need to have these interfaces approved giving sufficient notice so that it is possible to complete this procedure prior to the commercial roll out of ENUM. It is up to the individual TSP to decide if they wish to be involved in this process.

11.2.1.1 Interface between the AA and the TSP – Interface D

This has not been defined. Although it is thought that direct involvement in a Number Portability (NP) process may be a workable model it is sensible to consider other methods such as the use of XML, Radius and/or LDAP over a secure interface to a participant in the NP process. The goal is to construct a robust system that is easy for all parties to implement at a minimum cost.

11.2.1.2 Why are the TSPs not the AAs?

Although there is no barrier to a TSP offering AA services, they may not be willing to authenticate numbers provided via other providers. As such it would be necessary to have other AAs who are not TSPs in order to authenticate numbers from non-participating TSPs. Separating identification and validation allows a number of “mix and match” solutions for numbers that are not administered by a participating TSP. The

separate AA tier also provides for competition in this vital segment, which is intended to lead to lower costs for Registrants.

11.2.1.3 Can a TSP choose which AAs to work with?

TSPs would be required to work openly and on a fair commercial basis with all accredited AAs in order to be classed as participating. In order to make this viable a rigorous accreditation process is proposed (see Annex E); this will also ensure that suitable audit trails are maintained in order to prevent and resolve misuse issues.

11.2.2 How much will Authentication Cost?

If a TSP decides to participate in the trusted authentication process, that TSP has to provide authentication data and service at a reasonable cost. It will allow the ENUM Registrant to authenticate successfully the number without undue costs. It will be responsibility of the suggested UKEPG to monitor and ensure TSPs and any other source of trusted data required for authentication, provide their services and data at a reasonable cost and do not act in a way that may negatively affect the services offered by the Authentication Agency that is ultimately the entity responsible for authentication.

11.3 Combined validation and identification solutions (Trusted)

All of the following solutions are considered to be a trusted method of authentication as the TSP is the prime data source for the verification information.

11.3.1 Direct query to Registrant's TSP

This solution requires an independent bespoke solution to be designed and agreed between the TSP, the AA and either the Registrar and/or Registrant. A TSP may use the TSP account code as means of V&I or may use some other secure process.

The advantage of this solution is that a robust authentication takes place by the owner of the prime trusted data source i.e. the customer's TSP. The disadvantage is that it relies on the customer's TSP participating in the ENUM space.

11.3.1.1 Example query to Registrant's TSP - Interface D

For the trial, we have provided a simple model to mimic how a small TSP could participate. We send the relevant customer data, requesting a cryptographic hash from the TSP. If the TSP provides a matching hash, the Registrant is validated.

Example of information sent across D to TSP:

Name: Joe, Bloggs

Address: 10 Nowhere Road, Endsville, Surrey, KT1 1AA

Example of information sent across D to AA - TSP returns 160 bit SHA-1 Hash over (Name, Address, Phone No.):

4d42f5ef4054b6afadc692c7306579eb46d7d607

If the passed hash matches with the AA's hash over their copy of (Name, Address, Phone No.), a valid response is returned.

This method is quite strong as it uses only the information sent to a DQ database, but as the TSP already knows the phone number of the Registrant (from internal records), provides two levels of checking: correct phone number and hash.

11.3.2 Hook into number portability process

Every UK telephone number should be portable. Therefore, in principle, a number portability process exists for every number. In order to port a number the parties involved must first ensure that the customer requesting the port has been assigned that number. This is the same check that must be implemented before a Registrant can register an ENUM.

The number portability process may use the TSP account number along with the name, address and telephone number to validate and authorise the export/import of a number.

The Trial Group have had informal talks with the Number Portability Industry Group and have agreed that, in principle, the NP process could be enhanced to answer a query along the lines of “don’t port the number, just check these details match”. However, this would be a manual process. Although preferable, an automated system would have implementation costs and may therefore be more of an issue.

The introduction of the Carrier Pre-selection Service provides another mechanism that may be adapted to serve this purpose, at least for those TSPs that have Significant Market Penetration and so must support the service.

11.3.3 Issues and the way forward

A number of issues remain unresolved with the combined authentication solution.

11.3.3.1 Use of TSP Account Code

The Trial Group has identified an issue with the disclosure of the Registrant’s TSP account code to a third party (i.e. the Authentication Agency and/or Registrar). In principle the TSP account code is a secret that should only be known to the customer and the TSP. Disclosure of this ID to the Registrar and Authentication Agency (unless the AA is the TSP) remains an issue.

The TSP that provides service for a particular number to a customer may consider the account number to be privileged information to be used internally and shared only between themselves and the customer - this is its use as a Validation proof.

However, if this information is passed via a Registrar and a (potentially third party) Authentication Agency in a transparent form, then it has been exposed to those third parties and might be considered to be weakened as a validation proof in this process.

There are risks in transfer of this account number in a transparent form. The entities receiving this can store it and use the data to act on their own behalf without further TSP customer involvement or requests.

One option is to ensure that they are covered by the same duty of confidentiality as the TSP itself. This would (at least) require a strong enforcement procedure as part of the Registrar (and AA) accreditation process. In short, the intermediaries are instructed not to misuse the data.

Another option is to not pass the customer account code directly via intermediaries as part of the validation process. Instead, a secure code based on the account data and a secret selected by the TSP could be used; thus a secure hash over the customer account

data would be passed via the Registrar and AA, and that could be decoded only by the TSP on receipt. This raises the question as to how the aspiring Registrant generates this secure code.

In practice, a number of TSPs likely to participate in the validation process already have online bill viewing web services. For these, generating a secure hash to be used by the customer in subsequent registration requests would be a very minor addition to these services. It does add an initial step for the aspiring Registrant - logging into a bill viewing web service provided by their TSP to collect a code that can be passed in a registration request. However, this allows the data to be passed in an opaque format, maintaining data confidentiality whilst still allowing it to be used for Validation.

Whether a requirement placed on the Registrar and AA not to misuse the Customer Account Code is considered acceptable, or instead the participating TSP generates a secure hash for their customer to use is an interesting policy question that should be included in any consultation process. There is a “trade off” between security and cost. There are precedents in the existing Number Portability and Carrier Pre-selection Service processes (particularly the latter, as there is now an automated system to allow activation). Choices for ENUM need not be more stringent than those made for other processes.

11.3.3.1.1 Example using V&I method provided by a TSP

Vodafone has a Common Registration Platform (CRP), which enables their customers to be validated and authenticated. They then are given a user name and password to use to register for any of the Vodafone services.

The CRP registration works as follows:

- i) Customer logs onto Vodafone web site.
- ii) The user enters the mobile phone number.
- iii) An SMS message is sent with a security code (to determine possession of phone).
- iv) The user enters the security code.
- v) The TSP billing number is requested (to determine billed customer).
- vi) User enters: Name, date of birth, address and password for CRP registration.

It would be a logical extension of this process to then supply the Registrant with a token, which can be passed to the AA via the Registrar. The AA would use this token to confirm the details with the TSP. The token should have certain “time to live” for security reasons and to stop duplicate registrations.

Note that if the customer has used the CRP for another service, then they would only need to enter their existing user name and password to get the token for ENUM.

11.3.3.2 Automated Hook into Number Portability or CPS Processes

The Trial Group agreed that although a mimic of the commercial process should be tested during the trial, a true implementation of any envisaged fully automated process cannot be progressed until either ENUM moves to a commercial phase or there is some compelling reason for any potential external group to choose to participate in UK ENUM. If the participation of some external group is formalised the next steps may be as follows:

- i) Design and agree a manual process with the group
- ii) Evaluate and discuss options for an automated link into the process

11.3.3.3 Queries from non-TSP Entities

At present the UK number portability processes are run and operated by the TSPs that have subscribed to a bilateral porting agreement. Some TSPs are not subscribed to this process so this removes the opportunity to authenticate their customer numbers via this method. However, more importantly, it was a requirement of the UKEG that the role of Authentication Agency is open for competition. Since the NP process is not open to non-TSPs this ENUM requirement cannot be fulfilled by any such proposal as of yet.

Should this method be progressed then access to the NP process by non-TSP entities will need consideration and industry agreement. This also reflects heavily on any accreditation of ENUM entities that is proposed.

It is envisaged that these restrictions be addressed as and when a new process is designed, either by AAs being accepted to participate directly or via a TSP acting as their agent.

11.4 Separate Identification Solutions

During UKEG discussions it was felt necessary to avoid solutions that required any TSP to be involved and so the following identification solutions were proposed.

11.4.1 Send PIN/password to address (Trusted)

The entity performing the identification stage would send (through the post) a PIN or password to the Registrant's address. The Registrant would then use the PIN as proof of name and address, as the information would have been posted to the Registrant directly. Similar processes are today in use to validate the identity of (for example) credit card holders and Internet banking users, and have proved to be reasonably safe and efficient.

The main advantage of this solution is that is not dependent on involvement of an external part (TSP). However, the need to send and use a password/PIN to complete the validation process is likely to make the process longer and more costly than a purely electronic solution.

11.4.2 Use credit card payment (Trusted)

During the ENUM registration phase if a credit card was used as a means of payment then a positive authorisation from the credit card company could also be used as proof and provide the audit trail for the connection of name and address. The main disadvantage of this solution is that it is dependent on the involvement of an external party and therefore could become more difficult and expensive.

11.4.3 Paper documentation identification (Basic)

The aspiring Registrant is able to produce some supporting documentation for their identity. This would be expected to be one of the generally accepted identification documents such as a utility bill or bank statement, passport or driving licence.

Then the Registrant's name and address details are taken along with the number (or range) they wish to enter into ENUM. In this manner, the Registrant is identified.

11.5 Separate Validation Solutions

In the previous section validation solutions have been proposed that tie a name to an address. In conjunction with this check the AA must also then tie the same name to a telephone number. The following validation solutions are proposed:

11.5.1 Use of paper documentation (Basic)

In order to validate a number, the ENUM Registrant is requested to send a recent paper copy of the telephone bill to prove that they have the right to use that number. In order to be sure that the telephone bill has not been forged, the AA should try to ring the number to be sure that the number is still active and assigned to the Registrant. In the case of a mobile number, the check could also be done by sending an SMS message.

The solution has the disadvantage that it needs the exchange of paper documentation and some interactions between AA and ENUM Registrant. There is also an issue of data protection and security as a result of the holding of paper copies of bills.

11.5.2 Use of DQ database (Trusted)

Checking the associated numbers/user names in the DQ database validates the right for a user to register an E.164 number.

The solution has the advantage of using an already publicly available service. The clear disadvantage of the solution is that only a portion of UK numbers is listed in the DQ system. Approximately 40% of UK numbers are ex-directory and only a small percentage of mobile numbers are listed. For some classes of numbers like DDI there is not necessarily an accurate match between number and an end user's name.

Example of DQ Database use:

The trial AA software sends (Name, Address and Postcode) to the DQ database. If the resulting phone number matches that supplied by the Registrant, then a Validated response is returned. For example, if the data sent were:

Name: Joe, Bloggs

Address: 10 Nowhere Road, Endsville, Surrey, KT1 1AA

Assuming that this matches an entry in the DQ database, then if the returned telephone number matches the Customer Submitted Telephone Number, a Validated response can be sent. This is not as strong as TSP Participation as the data requested is not as precise as with TSP Participation and DQ databases can be spoofed.

If an AA were to choose the DQ route to validate a Registrant's details there are now a number of Directory Enquiries companies offering services using the number range 118 XXX. BT is one of a number of 118 companies providing DQ services.

The Terms and Conditions of BT's 118 500 service clearly state that enquiries must not be used to provide a commercial service. UKETG has not investigated the Terms and Conditions applied by other 118 providers. Therefore it would be misleading to suggest that use of the 118 DQ services is free for commercial ENUM implementation.

The Trial Group is also unaware of any automated link for queries into any of the DQ companies. If the validation and registration process is to be quick and low cost an automated link should be investigated with individual 118 companies.

The database that provides the raw data to the 118 companies is known as OSIS and is provided through a licensing scheme to the 118 companies. If an AA required a link into the OSIS database then a licence may be necessary.

11.5.3 PIN Code Validation (AA process) (Basic)

Dependent on the type of number that is being validated (i.e. Voice, Fax, Mobile), a PIN Code is communicated to the number within an agreed time period. The Registrant could request this to happen when convenient, for example within office hours or only afterwards. In the case of a fax number this is trivial, as a Fax containing the PIN Code can be sent. With a mobile number this is also easy, as an SMS message with the PIN Code can be sent to the phone. Sending the PIN Code to a voice number would probably involve an automated announcement unit speaking the PIN Code to the Registrant. Once they had this code, this could be passed on to the AA as part of the validation process.

It may be possible to make the customer dial a specific number and validate on a reversed PIN Code and inbound caller ID to speed up the process. This may be useful if the DQ check is used but does bring in extra security risks.

In the case of a DDI range, this PIN Code will be sent for use with the first and last numbers within the range for registration. Note that this may require configuration of customer equipment to ensure these numbers are mapped to a service when the PIN Code is sent to them, Equally, if the suggested dial back procedure is used, it will be necessary to select the “expected” presentation number to be used when calling to the specific number.

11.5.3.1 Pin Code Validation Example

Data Sent for Normal Landline:

Name: Joe, Bloggs

Address: 10 Nowhere Road, Endsville, Surrey, KT1 1AA

Validation: CC Match

RegNo1: +441234000111

RegNo1_Type: Voice

RegNo1_Time: Evening

AuthType: Trusted

Data Sent for Mobile Number:

Name: Joe, Bloggs

Address: 10 Nowhere Road, Endsville, Surrey, KT1 1AA

Validation: CC Match

RegNo1: +4477701234567

RegNo1_Type: SMS

RegNo1_Time: Any

AuthType: Basic

Data Sent for Business DDI Range (block of 40):

Name: Bloggs Limited

Address: Unit A, Gray Business Park, Bland, Surrey, KT1 1AA

Validation: Invoice - Utility Bill

RegNo1: +441234000000

RegNo1_Type: Voice

RegNo1_Time: Any

RegNo2: +441234000039

RegNo2: Fax

RegNo2_Time: Day

AuthType: Trusted

11.6 Summary

A number of solutions exist to enable an ENUM registration to be authenticated. As there is no universal service obligation not all solutions are considered to be trusted. However in the absence of a trusted solution, basic solutions are considered by the Trial Group to be acceptable.

All the combined V&I solutions are considered to be trusted:

- Direct query to a TSP
- Hook into number portability or other industry process

The separate Identification solutions are categorised as follows:

- Send PIN/password to address - trusted
- Credit card - trusted
- Paper documentation - basic

The separate Validation solutions are categorised as follows:

- Paper documentation - basic
- Query to DQ - trusted
- PIN Code - Basic

12 ENUM Security Threat Analysis

UKETG worked on an analysis of the security threats and vulnerabilities in the proposed ENUM system. This proved to be over ambitious partly because the subject is so large and partly because of resource and time constraints within UKETG. For instance, it was not possible to carry out a threat analysis on financial transactions since no money changed hands during the trial. An outline document was produced for discussion but analysis is still ongoing; the interim attack model is shown in Annex I.

A number of threat scenarios and possible solutions were considered. These included various forms of spoofing: impersonating any of the entities involved such as the Registry, Registrar, AA, Registrant and so on. Most, if not all, of these attacks can be detected or prevented using the authentication, validation and accreditation schemes that UKETG has developed.

There are other threats beside those arising from forged or broken credentials. These include eavesdropping, bogus financial transactions and hijacking name servers. Tampering with DNS data is another potential problem though some of these concerns can be addressed by the use of Secure DNS, DNSSEC. Access control for a Registrant's NAPTR records is also a worry since these could be manipulated by an unscrupulous but trusted application. The potential and impact of data harvesting and denial of service attacks also needs to be considered.

13 ASPs and Trial Applications

There are two main kinds of Application Services that can be provided; Registration support services and Client support services. These services are provided to the Registrant (or subscriber) and to the ENUM Client user, respectively.

13.1 ASP Interfaces

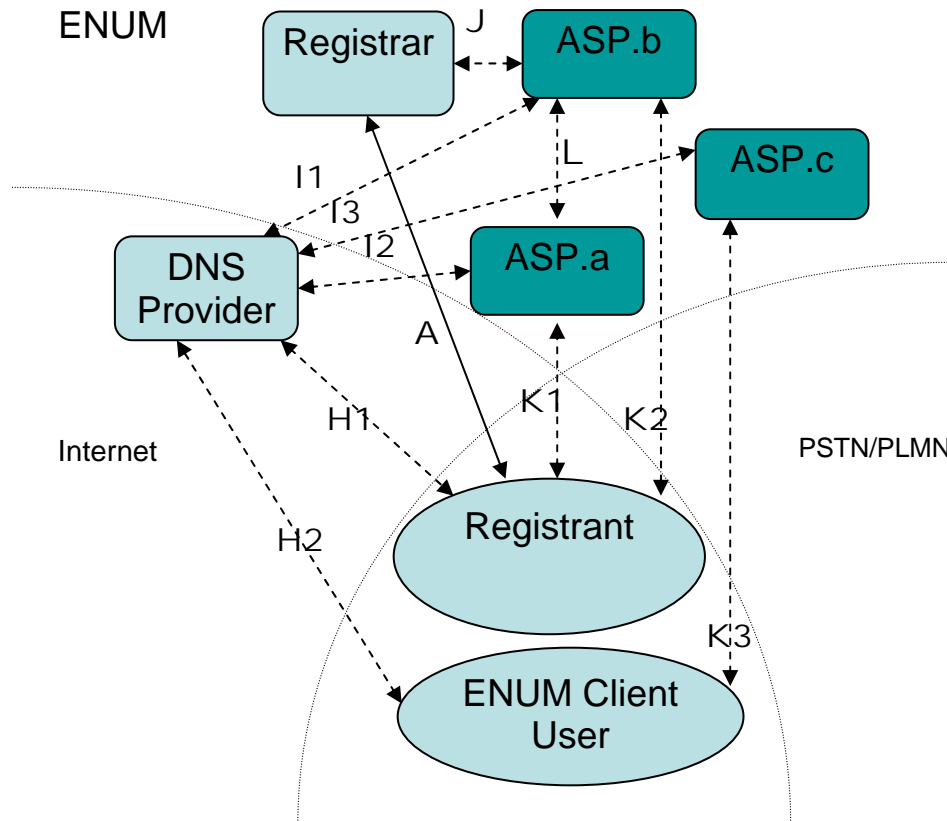


Figure 8 – ASP Interfaces

Although it operates in these two regimes, ASP can appear in three guises; the ASP may act as the agent for the Registrant, and if so may act as a front end providing support and coordination when populating or modifying the ENUM/DNS data for the Registrant (ASP.a), or they may support the customer during the Registration process (ASP.b). Finally, an ASP may act as an agent for the ENUM client end user (not the Registrant) when querying the ENUM data associated with a telephone number (ASP.c). The interfaces between the players are shown in the above diagram and are described here.

Interface K1 – Registrant to DNS Front End ASP

This interface is from a Registrant to their DNS front end ASP, and is used to populate and maintain the contact information that the Registrant wants to publish via ENUM. In effect, this is a direct connection from the Registrant to modify their records, rather than using one of their Internet Service Providers (e.g. an email provider) to modify this data

for them. It is assumed that the ASP acting as a front end for the DNS service provider gives a user-friendly interface by which contact records can be populated or modified by the subscriber.

Interface K2 – Registrant to Reseller ASP

A subscriber uses this interface when they want to use an ASP to arrange the Registration process for them. In this, that ASP acts as a reseller. The ASP will act as their agent to arrange the Registration Process, communicating with a Registrar and/or will arrange provision of a DNS Service Provider.

Interfaces J, I1 – Reseller ASP to Registrar/DNS Provider

This interface will be from an Application Service Provider to the Registrar and/or to the DNS Service provider. An ASP may be an agent for the Registrant during the registration process, acting as an intermediary between the Registrant arranging an appropriate Registrar and/or DNS service provider for their customer. This role is commonly called a Reseller.

Interface I2 – DNS Front End ASP to DNS Provider

This interface passes data to be stored by the DNS Service Provider in response to interactions with the Registrant or their agents. This DNS front end ASP provides a set of interfaces by which a Registrant or their agent can populate or modify entries, and the ASP can check the consistency of these changes, generate the equivalent DNS data, and pass this to the DNS Service Provider for storage.

Interface L – ASP to DNS Front End ASP

It is quite likely that other ASPs (operating in Subscriber mode, as an agent for the Registrant) will have to make changes to a subscriber's contact details (with their permission) mediated via a DNS front end ASP service that acts as an intermediary to the DNS Service Provider (as shown in interface I2), to obviate the concerns expressed in section 12.

Interface K3 – ENUM Client to Client Mode ASP

This interface is from an ENUM client user to an Application Service Provider in Client mode (i.e. one that queries for and uses the contact information stored in ENUM). For example, an email server might accept a mail with a telephone number as a destination address; it would query ENUM to find the email address associated with this number and could forward it accordingly.

Interface I3 – Client Mode ASP to DNS Provider

This interface is from an Application Service Provider (acting in Client mode) to the DNS Service provider to collect contact details that it will use as part of its Application Service.

13.2 Registration Support Service

In the former case, the application would be expected to interact with and act for the Registrant. However, where a range of numbers is registered by an enterprise, the application may also interact with a set of individuals within that enterprise.

There are a number of services that can be provided to the Registrant (or their organisation). Some will be purely intermediary, whilst others will include other ENUM services. For example, the ASP might provide DNS service as well as representing the subscriber in the ENUM Registration process (without being an accredited Registrar).

In many cases providers will already have a relationship with the customer. They may be able to provide ENUM services as well. For example, they may be able to arrange ENUM registrations for their existing customers, possibly including this as an optional component of the Internet access or telephony services they provide.

Examples of registration support services are:

- Financial - providing a payment scheme or credit arrangement not provided by Registrars directly (i.e. acting as a Reseller or Aggregator for ENUM registrations)
- User registration presentation - collecting and presenting the registration process with a particular user interface (e.g. a user-friendly web interface)
- User ENUM content presentation - providing a user-friendly web interface to support population and maintenance of Tier 2 DNS content for the Registration
- Combined service representation - arranging for Registration (via an accredited Registrar) and for DNS service to be provided to hold ENUM domain content for the registered number (or number range)
- DNS service provision - providing DNS service for the Tier 2 data related to a registration

13.2.1 Trial Experiences

During the trial it was found that validation and identification of ENUM registrations was non-trivial. Resolving the interplay of privacy requirements placed on service providers with the need to pass information onwards to different entities through what may be a chain of intermediaries has taken considerably longer than planned. Where an ASP acts as an intermediary, it is important to ensure that they have privacy policies that allow them to pass on those pieces of information needed for a subscriber's ENUM registration, whilst ensuring that they do not misuse this information for other purposes.

In the Registration process they act solely as an agent for the Registrant, and where they provide DNS service for Tier 2 ENUM data (or act as an intermediary to a third party DNS provider) they must ensure that adequate controls are kept over the person allowed to specify content for the Registrant's domain.

They must take reasonable care to ensure that only the Registrant can request that data be populated or changed within the ENUM domain they have registered, but equally must ensure that no indication of the identity of the owner of that domain is passed to others without the explicit consent of that Registrant.

From experience in providing an ENUM DNS content population and maintenance web service within an enterprise, it was found that, once the users populated their ENUM

domains with contacts, they rarely changed them. The users viewed the ENUM system as a way of publishing an Electronic Business Card with several telephone numbers and email addresses published under their main ENUM-registered telephone number.

What these users did do was to change the relative priorities between these entries, so that they could indicate which of the contacts was most appropriate at that time. This provided a kind of “Follow Me” service, but allowed the users to set email, SMS, or other non-interactive services as the best current priority. Whilst there were concerns with the volume of updates to the DNS data, it was found that these changes did not occur very frequently overall, so this is not seen as a major concern for DNS performance.

13.3 ENUM Client Support Service

Application Service Providers can also act for people without an ENUM registration. Once the data is published within the ENUM system, it is available for anyone to query and use. The entity making these queries and acting on the results is an ENUM Client. As this data is stored within the DNS system, any data appropriate to DNS can be stored and presented to querying clients. As such, a very wide range of Applications can include ENUM Client elements.

Some examples of these ENUM client services are:

- VoIP end systems that allow a caller to use a telephone number as a destination address; this can be achieved without ENUM, but where the caller and callee have VoIP service from different providers, can considerably simplify the process, and mean that the caller need not know whether or not their intended correspondent has a PSTN or VoIP end system (and, in the latter case, from which provider) in advance.
- ENUM can be seen as an enabler to cost-effective video calls and conferences over the Internet technology whilst retaining the familiar E.164 numbering scheme familiar to PSTN users.
- PSTN systems that can place a call to a destination using ENUM information. This means that the system can direct the call via an Internet voice gateway (if the Registrant has published an appropriate VoIP address). Alternatively, they can present it over the PSTN either using the initial phone number or another one gleaned from the returned ENUM contact information. Variations on this theme include the ability to indicate that a Registrant requires some specialised gateway to be invoked for communication, such as a speech-to-text relay system for those with hearing difficulties.

In addition, other applications are possible, such as:

- Web browser that uses a telephone number to address web sites
- Email service that allows telephone numbers to be used either as sources or destinations for messages and uses ENUM to find the email addresses
- Electronic Business Card application, that allows a set of contact addresses to be returned based on a single phone number
- Mobile phone browser (based on this Business Card application) to choose an appropriate means of communicating (e.g. selecting an entry indicating the Registrant’s preferred email, SMS or Instant Messaging address, and being

presented with a “compose message” window, or selecting the Registrant’s currently preferred phone, with mobile phone dialling this number.

- PC-based Address Book application that uses ENUM to retrieve up-to-date contact information; in this case the application can be integrated with VoIP client, web browser, and email client.
- Web service that presents contact information gleaned from ENUM to clients who query a phone number
- Hybrid telephony system, using ENUM data to provide new services. For example, caller display information from an incoming telephone call can be used to make a query of ENUM to search for web information associated with that caller’s number. This can be presented to the callee, so that if the web address included a picture and name, the callee could see this “on screen” as an enhancement over current caller display systems.

13.3.1 Trial Experiences

A simple Web lookup service has proved very popular. Similarly, the mobile phone-based ENUM client has been used extensively, and has been developed during the trial period. Privacy concerns (within an Enterprise) have proved fairly straightforward to solve using existing DNS technology. Different data was available depending on whether the ENUM query came from within the enterprise’s network or from outside – for example, TXT records holding the name of the user associated with a phone number were returned within the ENUM responses only for those inside the company (and using the company’s network).

ENUM-aware PSTN Internet Gateway/IP-PBXs have been introduced and have had a positive financial impact; calls are passed directly over Internet connections where ENUM queries show an appropriate VoIP end point address, without the need for coordination between the caller and callee organisations.

Although it has been possible to selectively route calls over the Internet for some time, attempts have generally been poorly co-ordinated and dependent on ad-hoc methods for rendezvous. When an ENUM system is used, this co-ordination is trivial. Control remains with the callee’s organisation, which drastically reduces management overheads and also greatly simplifies the use of Internet telephony. Using ENUM substantially reduces the response time for changing and publishing contact data. This problem becomes a simple matter of updating a DNS zone file and watching the DNS protocol automatically propagate those changes. Planning and Coordination costs are reduced using ENUM, as distribution of updated dialling plans is not needed.

In the trial system attached to Roke Manor’s PBX, the percentage of possible calls rerouted from the PSTN via an IP connection toward the end of the trial reached 20%; this reflected a strong “calling circle” and the availability of a corporate IP network. The major limitations were the lack of a public ENUM trial in Germany at the time of the tests, and corporate policies at some other major sites on firewall controls and connectivity of test systems to “mission critical” company PBXs. As well as the campus-local SIP phones, Roke Manor supported 14 SIP phones at fixed locations in other countries and 3 others that were assigned to nomadic users, all of which were provided with UK numbers for the test. The PBX at Roke Manor was configured to lookup these numbers in the ENUM system and use the reply to decide how to route calls for these numbers. This was used to make the PBX place SIP calls to SIP phones

and gateways anywhere on the corporate IP network (intranet). A user could dial a local extension and seamlessly have the call routed to any location on the corporate IP network, or the Internet. Roving users found this particularly useful.

The main result was that the system “just worked”; in a full production system, we foresee no problems at all. It seems certain from the trial experience that (at least for enterprises) there is a definite benefit to commercial rollout of ENUM.

13.4 Description of Trial Applications

MCI has participated as an Application Service Provider in the UK ENUM Public Trial. MCI’s application is entitled “SIP Service Interworking”. The purpose of this application is to demonstrate how ENUM enables end users on two disparate SIP “islands” to interwork directly over IP. Today, these disparate end points can only communicate through available PSTN gateways.

An associated test call sequence would be similar to the following:

- 1) CALLING PARTY (Provider X) dials +44 test number of CALLED PARTY (Provider Y) from soft client
- 2) Provider X SIP Server launches ENUM query for CALLED PARTY number
- 3) Internet DNS responds with ENUM results including URI of Provider Y SIP Proxy Server
- 4) Provider X SIP Server routes call to Provider Y network based on URI from ENUM DNS results
- 5) Provider Y determines availability and connectivity of the CALLED PARTY and conveys connectivity and protocol information to the CALLING PARTY via Provider X SIP Server
- 6) CALLING PARTY and CALLED PARTY may now communicate directly via IP connectivity

This application provides an excellent framework to illustrate some of the significant benefits ENUM provides, including total IP based connectivity and end user (CALLED PARTY) end user control of communications without privacy exposure.

13.5 Application Service Provider Testing Results

ASP: MCI

Application Name: SIP Internetwork Application

Description: This application demonstrated the capability to utilize ENUM queries for direct IP connectivity between disparate SIP service “islands”. Today, customers using different SIP services cannot direct connect to one another over IP. Gateway arrangements through the PSTN or other means are utilized in some cases, but these arrangements may incur transmission impairments through conversions or other difficulties. By launching an ENUM query, directly connectivity is possible between disparate SIP parties. Tests involving Web and email addresses in ENUM NAPTR records were also successfully executed.

The following are examples of successful tests utilizing UK ENUM trial resources:

DATE:	December 16, 2003
CC44 TEST NUMBER:	+44 1223 381001
ENUM URI:	sip:mciukenum1@nvta.globalipcom.com
ORIGINATING PARTY:	RICHARDSON, TEXAS-WINDOWS MESSENGER SOFT CLIENT
DESTINATION PARTY:	RICHARDSON, TEXAS-CISCO SIP PHONE
RESULT:	DIRECT IP CONNECTIVITY SUCCESSFUL
DATE:	December 16, 2003
CC44 TEST NUMBER:	+44 1223 381004
ENUM URI:	sip:mciukenum4@nvta.globalipcom.com
ORIGINATING PARTY:	RICHARDSON, TEXAS-WINDOWS MESSENGER SOFT CLIENT
DESTINATION PARTY:	RICHARDSON, TEXAS-CISCO SIP PHONE
RESULT:	DIRECT IP CONNECTIVITY SUCCESSFUL
DATE:	December 19, 2003
CC44 TEST NUMBER:	+44 1223 381005
ENUM URI:	sip:mciukenum5@nvta.globalipcom.com
ORIGINATING PARTY:	WASHINGTON, DC-WINDOWS MESSENGER SOFT CLIENT
DESTINATION PARTY:	RICHARDSON, TEXAS-CISCO SIP PHONE
RESULT:	DIRECT IP CONNECTIVITY SUCCESSFUL
DATE:	December 19, 2003
CC44 TEST NUMBER:	+44 1223 381006
ENUM URI:	http://iua2.net/enumber/
ORIGINATING PARTY:	WASHINGTON, DC-WINDOWS ENUM CLIENT/BROWSER
DESTINATION PARTY:	SANTA MONICA, CALIFORNIA-WEB SERVER
RESULT:	WEB PAGE CONNECTIVITY SUCCESSFUL

14 Accreditation

It is proposed that responsibility for accreditation will need to rest with the proposed 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.

14.1 Recommended scheme

UKETG considered a number of different schemes and these recommendations are made concerning the choice of accreditation scheme and its operation. The full discussion that leads to these recommendations is given in Annex E.

- 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 accept registrations only from Accredited UK ENUM Registrars.
- All UK ENUM authentication authorities will be required to comply with a scheme of accreditation approved by the proposed UK ENUM Policy Group. Once compliance has been self-certified, the Authentication Agency 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.
- The UK ENUM Registrar accreditation scheme and the Authentication Agency accreditation scheme is the responsibility of the proposed UKEPG.
- 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.

15 Legal Considerations

This section intends to provide guidance with regard to legal matters requiring consideration by companies who have or, intend to participate in the UK ENUM Trials, or its subsequent phases, to deliver ENUM related services to end user Registrants. It is intended to be of help and should not be assumed to be providing any form of legal advice on how any of the matters raised in this document may affect (and or may apply to) any particular organisation and or service. Independent legal advice should be sought if the reader needs such advice.

15.1 Overview

To date, the UK ENUM Trial progressed well throughout 2003 and (if agreed) is set to continue into 2004. The means by which was achieved, was under a framework provided by a Memorandum of Understanding for the UK ENUM Trial (MoU). This MoU was entered into by all UKETG Participants, and had the following key features and functions:

- Definition of the purpose and scope of Trial
- To define high-level architectural, technical, operational objectives and capabilities of the Trial.
- To defines general principles of participation with regard to promotion, competition, barriers of entry.
- To bind participants to principles of, co-operation, openness, fair trade, and general conduct with regard to data privacy, protection and competition.
- That the Trial is not for profit, and participants do not expect any financial benefits or compensation.

As a prerequisite to enable the transition towards a full Production or Commercial UK ENUM service, there may be a need for change with regard to the existing MoU, for (but not limited to) the following reasons:

- To implement and evaluate production quality platforms and systems.
- To clearly bring to an end, and then move away from Trial
- To implement and evaluate secure, stable, integrated platforms and systems as well as authentication and verification platforms and systems.

Of the five phases defined in the MoU all were completed and reported back to the UKETG. How the transition to a Production and / or Commercial ENUM phase should be arranged has yet to be decided. There are, as part of such a migration, requirements for full legally binding contracts and agreements between the various tiers of participation within and upon the Participants. At such time as the Trial includes Registrant participation then, for example, there will be important issues to be considered and decided with regard to fiscal remuneration, price, and other implications.

However at this stage it is undecided what form this transition could take. Various possible options include:

- By amendment to the existing Trial MoU
- By agreeing and subscribing to a new MoU for Commercial service, which covers and includes Production phase terms.
- By new MoU specifically for a Production phase.

Whichever vehicle of transition is adopted specific considerations must be given to encompassing the following:

- Degree of formality - the existing MoU is non-binding and voluntary.
- Existing Trial information, and level of confidentiality of any future documents relating to data collected, technical specifications and production systems.
- Intellectual Property and legal ownership, e.g. copyright, trade secrets, licences, patent applications.
- Continuing obligations, or surviving terms of Trial MoU
- Conduct under data protection and privacy laws.
- Conduct under competition and antitrust laws.
- Termination of Participation.

In addition to the above, the UK ENUM Trial, by definition as a medium that facilitates electronic communication is ultimately governed by both UK and EU legislation. See Annex F for details of Industry Wide considerations, and Annex G for ENUM participant specifics.

In summary of the above all UK ENUM Trial Participants and any future participants must give careful consideration not only to legal implications detailed in the two associated annexes F and G, and considerations for a successful UK Trial, but also from what has been learned to date and how that experience will affect hereafter any Production or Commercial phases.

Perhaps much more importantly, consideration must be given to where any parts of UK ENUM prove less successful, or where misuse of any part of the Registration or other processes may occur.

16 Open issues

Although UKETG made progress in several areas and has produced good work, the UKETG identified a number of open issues. These remain unresolved. At the time of writing, there is no consensus about how to proceed. It is possible that these could be explored in a future phase of the trial (if any) assuming that both UKETG and UKEG are willing to take that step. This section discusses these unresolved issues.

16.1 On-line authentication and validation

The UKETG was unable to develop an on-line system for the authentication and validation of registrations. This requires co-operation from a telephone company. Tentative discussions were held with the UK Number Portability Forum about how to build such a system. However these were inconclusive. A further difficulty was finding the resources to implement a prototype system.

For a production ENUM system, on-line authentication and validation is essential. This will be the only way to ensure registrations get processed quickly and at a reasonable cost. Paper-based mechanisms, currently used for the number portability process, would not be appropriate. Another benefit from testing a prototype system would be to get an idea of the actual costs of doing the authentication and validation checks. This is essential for establishing the overall cost of processing an ENUM registration. That in turn could be a significant factor in the uptake of ENUM by consumers.

16.2 Transfer of Registrations

No registrations were transferred between Registrars. This means that the necessary processes, procedures and interfaces are unclear. It should be relatively straightforward to implement and document these. This will also be a necessary component of a production ENUM service as it will enable competition and promote consumer choice.

16.3 Financial Modelling

All activity within the trial has been self-funding. No charges have been levied for registrations, DNS provision, authentication and so on. UKETG has not modelled or documented the likely financial transactions and money flows between entities. To some extent this was outside the original scope of the trial. However this work needs to be done before a production ENUM service starts. This activity could be accomplished in a second phase of the trial if it was agreed that charging was acceptable.

16.4 Authentication

The work on authentication and validation identified many examples of telephone numbers that proved difficult to verify. These included DDI blocks allocated to an organisation; premium-rate numbers; pay-as-you-go mobile phones; freephone and non-geographic local and national numbers. There appear to be no easy solutions for strong verification of these numbers. Ex-directory numbers also presented a problem.

During the trial, registrations were verified by manually checking against the BT Directory Enquiries (DQ) database. This was shown to be unsatisfactory for several classes of phone number such as the ones listed above. A long-term solution would appear to require co-operation from all telephone companies. A voluntary scheme would seem to be the best way to achieve this. However that presents a number of challenges, as telephone companies may not see any business case to justify an authentication system for their customer's phone numbers.

16.5 Secure DNS

The DNS is currently vulnerable to a number of spoofing attacks: tampering with replies, impersonating name servers and so on. These could be a serious concern for ENUM. For instance, telephone service for an ENUM registration could be spoofed or hijacked if an attacker manipulated its NAPTR records. The IETF is working on a protocol, Secure DNS or DNSSEC, to protect the DNS. This involves public-key encryption to digitally sign DNS data and verify those signatures.

Development of the DNSSEC protocol has not yet been completed by the IETF. However it appears to be close to a final standard. UKETG was unable to test DNSSEC since a completed standard was not available during the trial.

Assuming that standard is finally agreed, there are a large number of issues that will need to be worked on before DNSSEC could be deployed for ENUM. These include tools for signing DNS data and verifying those signatures, key management, data signing policies and procedures, introducing new keys and withdrawing old ones, assessing the impact on the Registry, Registrars and DNS providers of introducing DNSSEC. A great deal of work remains to be done in this area.

16.6 Threat Model

UKETG has recognised that considerable work needs to be done on a security analysis on an ENUM system; however, only some of that work has been carried out to date. A draft document was produced which lists some of the threats and defences. This is not definitive and more work is needed. An analysis of the threats to financial transactions and money flows will only be possible if these processes can be defined in some future phase of the trial.

17 Future of UKETG

The future of the UKETG is unclear. At the time of writing, it is not known if UKETG will continue. And if it does continue, decisions will need to be taken about what it will do and how the trial group would be organised. UKETG has had preliminary discussions about this. However no consensus has yet emerged. There is a general feeling that UKETG should continue in some form, though its scope and purpose are currently undecided. Discussions will continue within the trial group and also with UKEG, DTI and Ofcom. At this time it would be premature to speculate on the outcome of these discussions.

18 History of the Report

Version	Comments	Date
Draft A	Skeleton report	October 2003
Draft B1	More text added from existing UKETG documents	December 2003
Draft C	Input from UKETG members - major editing	December 2003
Draft D	Major editing as agreed at meeting on 4/2/04	February 2004
Draft D2	Reformat as agreed at 040218 Conference Call	February 2004
Draft D3	Final re-layout and minor edit per email exchanges	March 2004
Issue 1.0	Updated to reflect new ENUM RFC	April 2004
Issue 1.1	UKEG approved version	May 2004

Annex A – Companies and organisations active in the UK ENUM Trial Group

Observers:

- DTI
- Oftel

Meta-Registry:

- UKETG Chairman

Authentication Agencies:

- BT Exact technologies
- Vodafone

Registries:

- Internet Computer Bureau plc.
- Neustar
- Nominet

Registrars:

- Atlas Advanced Internet Solutions
- Afilias

DNS Service Providers:

- Nominum
- Atlas

Application Service Providers:

- Roke Manor Research
- MCI

Note that several companies also provided other services; for example, Atlas Advanced Internet Solutions acted also as a DNS Service Provider, and ICB also had Applications in this and other trials.

Also, note that due to the sensitivity of the Meta-Registry role, this was carried out directly under the control of the Chairman.

Annex B – Terms of Reference for the UK ENUM Trial Group

Responsibilities

UK ENUM Trial Group is responsible to set up and carry out the ENUM Trial with the aim to test architectural, technical, operational and user experience aspects related to the provision of ENUM capabilities, as defined in IETF RFC3761, for Country Code 44. Results collected in the trial will enable UKEG, and any other interested party, to gain information and experience on how to provide and implement ENUM capabilities in the commercial phase.

More specifically the objectives of the trial are:

- To produce interim and a final reports covering all aspects needed to meet the specified requirements of UKEG to identify technical and policy issues that need to be addressed prior to launch of a commercial implementation of ENUM within the UK and make recommendations based on experience gained during the course of the trial where appropriate.
- To evaluate processes/interfaces/protocols for the interactions between the different parties involved (Tier 1 Registry, ENUM Domain Name System (DNS) Provider, ENUM Registrar, Application Service Provider, Number Assignment Entity, Authentication Agency and Telephone Service Provider).
- To determine technical and operational requirements to provisioning ENUM records at Tier 1 Registry and ENUM DNS Provider level and assess DNS requirements/ implications in the provision of ENUM services;
- To test from a technical and user perspective applications based on the use of ENUM capabilities.
- To evaluate and refine economic benefits and costs of supporting ENUM.
- To consider and implement where appropriate inter-working capabilities with other
- ENUM trials.

The UK ENUM Trial group is an independent industry group working in close cooperation with UKEG Group.

Operational, technical and administrative issues related to the ENUM Trial are under the direct responsibility of the UKETG. The UKEG will act as the Steering Committee, closely following the developments of the trial, giving strategic guidance and solving possible conflicts between the participants.

Trial evaluation will be carried out during the period of the trial and it is expected that key learning points will be identified on an ongoing basis. UKETG will make interim reports available to the UKEG. At the conclusion of the trial a final report will be drafted summarizing the experiences learned and, if appropriate, putting forward recommendations for the implementation of the ENUM commercial phase.

Membership

The UK ENUM trial group is open to DTI and all organizations that are active participants in the ENUM trial.

Members of UKETG must sign the trial MoU that sets out the trial principles and objectives, identifies roles and responsibilities of the participants and provides the administrative and operational framework for trial activities.

All participants in the activities of the UKETG will underwrite their own expenses and associated costs in participating in the trial. Neither compensation nor direct financial benefits are foreseen for any trial participant.

Method of Working

All parties participating in the trial must co-operate in accordance with the rules defined in the trial MoU. Decisions will be taken by consensus (consensus is defined as “lack of sustained opposition”) amongst the trial participants, with the involvement of the UKEG if appropriate.

The UKEG will monitor the activities of UK ENUM Trial group, giving strategic guidance and solving possible conflicts among trial participants.

Jim Reid (Nominum) and Marco Bernardi (NeuStar) have been appointed Chairman and Vice Chairman of the group.

Trial Managers have also been appointed as it is recognised that the success of the trial will also depend on an adequate level of management of technical and financial resources, coordination amongst the participants and communication between the trial group and UKEG.

The Trial Managers are:

- Marco Bernardi (Neustar) – Co-ordination of trial group reports and outcomes, facilitation of communication within the trial group and with the wider UKEG group
- Lesley Cowley (Nominet) – Budget Management
- Paul Mylotte (BText Technologies) – Project Planning and Monitoring.
- Jim Reid (Nominum) – Technical and Operational Management

The Chair and Vice Chair will have a duty to carry out chairing functions impartially. Where the Chair/Vice chair also represent interested organisation, they will clearly indicate when they are acting in the role of Chair, and when they are acting on behalf of their organisation.

The Trial Managers have to follow the same conduct in the fulfillment of the their roles.

ENUM UK trial meetings will be held regularly and an email distribution list of contacts from eligible organisations that are part of the trial will be maintained.

ENUM UK Trial Group may decide, if appropriate, to established informal ad hoc sub groups to deal with particular issues.

Trial Documents

- All material jointly produced within the trial phase will be deemed 'Trial Material' and will remain subject to consensus agreement within the UKETG prior to release to the UKEG or any other party, as specified within the terms of the MoU.
- UKETG should inform UKEG of progress at regular intervals, periods to be agreed between UKEG and UKETG once milestones dates for the trial have been developed, or when specifically requested by UKETG.
- It is recognised that some trial material would need to be exchanged with other parties if trial inter-working is to be considered. Such information should only be supplied if deemed necessary to meet specified requirements between the trial parties involved. The level and detail of information exchanged will be subject to consensus agreement within the UKETG, prior to any action.

Annex C – User Memorandum of Understanding

Introduction

Enum is a system for bringing together telephone numbers and Internet domain names and ‘Internet Protocol’ (IP) numbers.

For more information about what ENUM is, see the help sheet “*What is ENUM? What can I do with one?*”

ENUM was designed by the international technical group called the Internet Engineering Task Force. At the moment the UK E-Num group (UKEG, a collaboration of telephone, internet and academic organisations) is running the UK trial of the system. Various member organisations are participating on a voluntary and unpaid basis to experiment with the technology and system.

Nature of this Document

This document is the ‘Memorandum of Understanding’ (“MoU”). It is not legally binding. Because it is not legally binding, neither you nor the members of the UKEG can enforce this agreement in a court. However, this MoU does explain your role in the ENUM system and includes matters to do with Data Protection and what we will do with your data, so you should read it carefully. We will not sell your data or use it for junk mail, although it is possible you will receive communications from a member of the UKEG other than your Registrar about the trial. The members of the UKEG have also written a memorandum of understanding to describe how they will deal with each other. That is also non-binding.

Note: your Registrar may in addition have legally binding terms and conditions in relation to the services they provide to you and payment for those services. These charges are not for ENUM but for ‘normal’ things like email or telephones.

The System

1. You are a user of the UKEG Trial Enum system, which is operated by several organisations. You will deal with your Registrar, and will not normally deal directly with any of the other organisations running the system. As a user you will be applying for an ENUM record, so any reference to ‘an ENUM’ is a reference to a record in the ENUM system.
2. Because this is a trial system you should only participate if you understand and accept that:
 - 2.1 the system may be changed or discontinued at any time, so that you should not rely on it being there in the future;
 - 2.2 as a trial system, THE UKEG AND PARTICIPATING PARTIES IN THE TRIAL ACCEPT NO LIABILITY OF ANY KIND TO ANY PERSONS IN RELIANCE ON THE ENUM (to the extent permissible by law) and no guarantees or warranties as to quality, fitness for purpose or satisfactory levels of service or operation can be assumed or relied on;

- 2.3 everyone running and involved in the UKEG trial is doing so on a voluntary basis as part of an open experiment, so information about the number of users, types, any documents relating to your registration and all other information may be made available to everyone within the UKEG (but the members will abide by data protection law);
- 2.4 you should share with UKEG your experiences of the trial, and you will not be able to keep any information about your experiences or involvement with ENUM confidential;
- 2.5 any ENUM registration now will not give you any priority or special status in any future ENUM system, whoever operates it and you should not try to block any future final system;
- 2.6 an ENUM has no legal existence, is not an item of property, and you have no rights in it or over it and that, if for any reason the courts decided that an ENUM was an item of property, you disclaim any beneficial interest in it;
- 2.7 no one can claim any rights or ownership in any part of the ENUM system on trial, including domain names, telephone numbers, copyrights or other intellectual property rights, or the ENUM registrations themselves by reason of their involvement in the trial; and
- 2.8 you can have no commercial or proprietary interest in participating in the trial which you may only participate in for non-commercial reasons.

The Participants

Users

3. You are the Registrant. In order for the ENUM system to work you must:
 - 3.1. apply for an ENUM;
 - 3.2. have targets (e.g. telephone number or email) for the ENUM to point to (note that although the ENUM will be a UK ENUM i.e. have the 44 number for the UK, the telephone number does not have to be a UK number and the domain name does not have to end .uk);
 - 3.3. be prepared for the telephone number to be available to the public (i.e. not ex-directory);
 - 3.4. deal with your Registrar, rather than the other participants in the system;
 - 3.5. submit all the information required for the registration and/or requested by your Registrar;
 - 3.6. promptly notify your Registrar of any changes in that information (for example, if your address changes);
 - 3.7. keep any passwords or identifying codes given to you by your Registrar secret and secure;
 - 3.8. give the data protection consents explained in paragraphs relating to Registrars and Registries;
 - 3.9. there is currently no charge for a trial ENUM registration, so you do not need to pay, and no one will pay you, although if the ENUM system became permanent you may have to pay in order to gain or keep a registration;
 - 3.10. notify your Registrar if any legal dispute arises about the registration or part of it (e.g. just the domain name);

- 3.11. ensure that any telephone number given remains in service and that any domain name server responds authoritatively to requests for the domain name at all reasonable times;
- 3.12. not do anything which would be in breach of third party intellectual property rights, or use someone else's domain name registration or telephone number in your ENUM record;
- 3.13. if requested, let your Registrar or the UKEG know about your experiences of using the trial system – if you do not like it, say so, and why.

Registrars

4. The Registrar is your main contact with the ENUM system, and they will also deal with the Registries, as your agent, where necessary.

The Registrar's role is:

- 4.1. to be the main commercial contact with you, deal with the customer service matters;
- 4.2. depending on the Registrar's business model they will may provide the domain name services (email, websites etc.), allow you to specify your own, or offer you the choice of buying these services from their commercial partners or operate some other scheme;
- 4.3. to provide you with a suitable means to access information about ENUM services and the registration process;
- 4.4. explain the terms of the ENUM service (currently, just the details of this MoU) to you;
- 4.5. provide you with the means to make and update a registration (in conjunction with the Authentication Agency);
- 4.6. deal with the Authentication Agency (or in some cases, the Registrar may fulfil the role of the Authentication Agency);
- 4.7. arrange (possibly in conjunction with the Authentication Agency) a system to allow you securely to identify yourself to the Registrar ;
- 4.8. provide a mechanism to allow you to alter the records for each ENUM registration (strictly, the 'NAPTR' records);
- 4.9. comply with Data Protection legislation, which means that you must give them permission to use your personal data for the purposes which they explain to you;
- 4.10. to pass information about the ENUM trial to the UKEG; and
- 4.11. to be your agent in dealing with the appropriate Registry.

Registries

5. There are 3 organisations running the Registry, each looking after its own different part.

The Registry will record the details of your registration, including:

- 5.1. the name of your Registrar;
- 5.2. the ENUM
- 5.3. your name, address, telephone number, fax number and contact email;
- 5.4. details of an administrative contact;
- 5.5. details of a technical contact; and
- 5.6. details about the internet name server computers for the registration.

6. Some of the information held by the Registry is 'personal data' as defined by the Data Protection Act 1998. In order to have an ENUM registration, you must give your consent to your personal data being held this way and used for purposes related to the operation of your ENUM registrations (which may include sending this information to other countries which do not have such strict data protection legislation). If you submit an application, you are giving these consents and appointing the Registrar as your agent to pass the information and the consents on to the Registry that is holding your registration.
7. In order that you can give your consent, you should know who the Registries are:
 - 7.1. GEOGRAPHIC: for telephone numbers starting +4414, +4415, +4419 and +44208 the Registry is Nominet UK, the UK Internet Names organisation;
 - 7.2. MOBILE: for telephone numbers starting +4477 then (3 to 9) the Registry is Nominet UK; and
 - 7.3. OTHER: for telephone numbers starting +4480, and +449 the Registry is Nominet UK.
8. There is currently no publicly available ENUM directory or WHOIS service or equivalent, but such a system may exist in the future. The default position is that your name will appear on such a service. Details will be made available in the event that such a service is introduced.
9. The Registries will not be able to hold your data if you withdraw your data protection consent, and therefore you will not have an ENUM.
10. The Registries have a discretion to alter, suspend or cancel records if they need to do so for reasons of good Registry practice, to correct errors in the register, if you withdraw your data protection consents, or if their involvement in the trial ends or alters.

Authentication Agency

11. The Authentication Agency's job is (in summary) to try to ensure that people are who they say they are; and the domain names and telephone numbers they give are actually theirs.

They will do this in conjunction with the Registrars and in some cases the same organisation may fulfil both roles. Your Registrar will be able to tell you this.

DNS Provider

12. DNS means 'Domain Name System'. Domain name registrations are used on the Internet to allow humans to remember the address numbers of computers. The DNS Provider may be your Registrar, or may be someone else you have specified to operate your email and websites. Under the UKEG trial they have certain technical obligations that do not need to be set out here, but include looking after the actual records for the ENUM (as opposed to the existence and location of those

records, which the Registries do). They also have a duty to report to the ENUM group.

Application Service Provider (ASP)

13. The ASP will be providing you with applications. The ASP may also be your Registrar and/or your DNS Provider. The ASP may need to tell you what should be in your ENUM record (NAPTR record) but will not be able to change it themselves (unless they are also your DNS Provider).

Although this document is not legally binding, please sign it to confirm that you have read it and understand the nature of the ENUM trial and its limitations.

Signature: _____

Print Name: _____

Print Position [e.g. Director]: _____

Signed on behalf of [Company etc.]: _____

Annex D – Administration of the Meta Registry for 4.4.e164.arpa

1. The UKETG Chair will operate the meta-registry for *4.4.e164.arpa*. Updates to this zone will only be made with the unanimous approval of the Trial Tier 1 providers. In the event of a dispute, UKETG will decide.
2. UKETG Chair will ensure this meta-registry function operated for the duration of the trial and will co-operate fully with any transition to a production service if or when this occurs.
3. The meta-registry operator will be responsible for all updates to the RIPE database for the duration of the trial. These will be subject to unanimous consent by the Trial Tier 1 providers.
4. During the trial the meta-registry will assign number blocks or area codes or some other appropriate and mutually agreed addressing unit of telephone numbers to Trial Tier 1 providers. The Trial Tier 1 providers will determine with the meta-registry operator what those assignment units will be and how they are allocated between the providers.
5. During the trial the meta-registry will be prepared to reassign number blocks or area codes or some other appropriate unit of telephone numbers among Trial Tier 1 providers. The Trial Tier 1 providers will determine with the meta-registry operator when and how this reallocation will take place. All UKETG members will be informed of the reallocation of number blocks in a timely manner.
6. The meta-registry operator will perform all update requests in a timely and efficient manner.
7. The Trial Tier 1 providers can request UKETG appoint a replacement meta-Tier 1 Registry operator.
8. If the meta-registry operator resigns or fails to adequately fulfil that role, UKETG can choose a replacement. The incumbent will co-operate fully with the transition to that replacement.
9. This note is subject to review by UKETG in light of operational experience.

Annex E – Accreditation for UK Production ENUM

E.1. 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 Authentication Agency 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.
- 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.

E.2. 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 Domain Name System 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 Authentication Agency 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 / Authentication Agencies. 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.

E.3. 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 Authentication Agencies (AA) and telephone service providers (TSP), and co-operation between organisations in these roles and the avoidance of avoid anti-competitive and monopolistic practices will also need to be addressed.

E.4. 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.
- 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.

E.5. 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.

E.6. 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 Authentication Agency should be accredited for UK production ENUM.

E.7. Roles to be Accredited

E.7.1 Registrar

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

E.7.2 Authentication Agency

An Authentication Agency 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.
- 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.

E.8. 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.

E.9. Recommendations

E.9.1 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.

E.9.2 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 Authentication Agency 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.

E.9.3 Accreditation Scheme Oversight

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

E.9.4 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.

Annex F - UK ENUM Legal Considerations – Industry

High level Industry-wide Considerations

Overview of current relevant UK regulation (UK regulatory regime for ENUM):

On 25 July 2003 the UK implemented a new regulatory framework for the regulation of electronic communications. In addition, parts of the Telecommunications Act 1984 were repealed. The new regulatory framework is based on new EC Communications Directives that are intended to converge and harmonise communication regulation throughout the EC.

This package of Directives introduced a new framework and regulatory regime that saw the ending of the licensing regime and the move to general authorisation.

The five new Directives are:

- Directive 2002/19/EC - on access to, and interconnection of, electronic communications networks and associated facilities (the Access Directive);
- Directive 2002/20/EC - on the authorisation of electronic communications networks and services (the Authorisation Directive);
- Directive 2002/21/EC - on a common regulatory framework for electronic communications networks and services (the Framework Directive);
- Directive 2002/22/EC - on universal service and users' rights relating to electronic communications networks and services (the Universal Service Directive); and
- Directive 2002/58/EC - concerning the processing of personal data and the protection of privacy in the electronic communications sector (the Privacy Directive).

The Telecommunications Act 1984 was replaced as the primary legislation for the regulation of communication providers by the Communications Act 2003.

The Communications Act 2003 implemented the first four of the five Directives above. The fifth is being implemented separately in the autumn of 2003 by Statutory Instrument (SI No.2426 of 2003).

The new regime aims to be “technology neutral” and is applied to all electronic communication services and networks. Under the new regime communications providers can provide services and networks without first having to seek permission or authorisation. Instead of a set of licences with varying obligations, all communications providers now have to abide by the General Conditions of Entitlement and any specific conditions that individually apply to them.

The General Conditions are a set of 21 conditions outlining the minimum obligations of communications providers. As providers do not and will not receive a licence that sets out their individual conditions of operation, it is recommended that all UK ENUM Trial Participants should read the General Conditions carefully, and potential application providers so that service providers may determine which of the conditions apply to

them. Note that each of the General Conditions contains a definition of the type of communications provider to which that General Condition applies.

The General Conditions can be found at:

http://www.oftel.gov.uk/publications/eu_directives/2003/cond_final0703.pdf

For further information on the background to the new regime refer to the Of tel website at:

http://www.oftel.gov.uk/ind_info/eu_directives/index.htm

A guide to the new regulatory framework for service providers can be found at:

http://www.oftel.gov.uk/publications/eu_directives/serpr1202.htm

The Statutory Instrument implementing the Privacy Directive can be found at:

<http://www.hmso.gov.uk/si/si2003/20032426.htm>

At present, the following five organisations are involved in the regulation of electronic communications:

- Oftel,
- Radiocommunications Agency,
- Independent Television Commission,
- Radio Authority, and
- Broadcasting Standards Commission

On 29 December 2003 these organisations merged to form one regulatory body for communications, The Office of Communications (Ofcom).

More information about Ofcom can be found on the Ofcom website at:

<http://www.ofcom.gov.uk/>

Annex G – UK ENUM Legal Considerations - Participants

Specific Obligations

UK ENUM Trial participants may also benefit from giving due consideration to the following specific obligations as may apply to their activities under the Trial MoU or moving forward into a Commercial phase of the Trial:

1. General Condition 1.2 of Communications Act 2003

General Condition 1.2 requires that:

“where [a] Communications Provider acquires information from another Communications Provider before, during or after the process of negotiating Network Access and where such information is acquired in confidence, in connection with and solely for the purpose of such negotiations or arrangements, the Communication Provider shall use that information solely for the purpose for which it was supplied and respect at all times the confidentiality of information transmitted or stored. Such Information shall not be passed on to any other party (in particular other departments, subsidiaries or partners) for whom such information could provide a competitive advantage”.

Furthermore,

2. The Communications Act 2003, provides conditions relating to and for:
 - Customer Interests – Sections 52, 53, 54
 - Universal Service – Section 65
 - Competition Legislation – Sections 369, 370, 371
3. The Data Protection Act 1998 provides principles and conditions relating to sensitive personal data.
4. The Competition Act 1998 provides principles and conditions relating to fair trade, and abuses of dominant position.

(These are dealt with in more detail below)

Other considerations for UK ENUM Participants

Firstly, it should be noted that much subsequently referred to is dependant of the outcome of the Trial Phase, and / or any final operational policies, yet to be adopted in the UK.

Each participant will also need to give due consideration to the specific legal ramifications and implications of each role undertaken by them. As such where all previous inter-working arrangements have been governed by the terms of the existing MoU, of which some terms may continue to apply in whole or in part as the UK trial moves into a production or commercial phase, much that is now envisioned is either specifically prevented under MoU or not covered by it at all.

Furthermore there will be a need, in due course, for new and additional participant agreements / contracts to govern each separate and definable commercial and non-commercial arrangement. The legal considerations shown here are envisioned as

probable minimum requirements and are not fixed in any way at this stage. The outlines below adhere to the consensus structure and nature of expected participant roles of the UK ENUM Industry. Specifically for Commercial phase ENUM where Participants should make use of such contracts and agreements to guarantee amongst other things, service levels and dispute resolution procedures and so on.

Where separate legal agreements are needed, and the purpose of such contracts and subsequent contractual relationships, should be considered as a continuous part of the UK ENUM Trial as they progress and have been summarised into the following categories/roles:

1. UK ENUM Policy Group (UKEPG)

The UK ENUM Policy Group is expected to be a formal legal entity able to function fully in the commercial domain, and which will be responsible for the introduction, development and enforcement of regulations and policies, codes of practice, accreditations*, and accreditation schemes*. The UK ENUM industry is anticipated to be self-regulating. *N.B. * Where this document refers to accreditations, it should be noted that the who, how, and against what criteria and upon what legal basis, is the subject of the Accreditation For UK Production ENUM document (in Annex E)*

It is currently proposed that the UKEPG is to be made up of a interoperating forum of management and stakeholder groups, as well as other groups including representation by public forum, and is envisaged to have a secretariat. The UKEPG therefore falls outside the scope of this section of the report, otherwise than where it is expected it may have legal duties/rights or other obligations that may impact on the legal and contractual relationships referred to between participants (including any financial considerations) below.

The UKEPG will accredit, appoint and contract with the Tier 1 Registry. The UKEPG will accredit and enforce compliance with Tier 2 Registrars and separately also with the Authentication Agencies. The UKEPG may be part or wholly financed by the trading activities of UK ENUM Participants.

2. Tier 1 Registry

The Tier 1 Registry will manage the UK ENUM authoritative database of *4.4.e164.arpa*. domains.

As the Tier 1 Registry, will operate at the appointment and with the accreditation of the UKEPG, and in accordance with the applicable policies and codes, then the Tier 1 Registry requires a contract with the UKEPG. Such contract should enable and facilitate the Tier 1 Registry to in turn contract on an equal opportunity basis with Tier 2 Registrars.

3. **Tier 2 Registrars**

Tier 2 Registrars are entities who collect information relevant to the registrations of ENUM domains and who organises the registration on behalf of Registrants (both corporate and individual).

As successful registrations will require both interactions with a UK ENUM Authentication Agency, and the facilities to provide updates to the Tier 1 Registry, the Tier 2 Registrars are envisioned to operate under the accreditation of, and in conformity to, the codes of the UKEPG. Furthermore, Tier 2 Registrars will be required to interoperate, at the request of Registrants who wish to transfer ENUMs between Registrars.

Tier 2 Registrars will need to contract separately with the Tier 1 Registry, possibly other Tier 2 Registrars (depending on Tier 1 – Tier 2 Contracts) and end user Registrants.

It is at this point, (i.e. the point where an end user Registrant places a order with a Tier 2 Registrar, and the billing relationship resides) that the end user Registrant's Contract sits and that the majority of legal issues and points of consideration therefore arise. With specific regard to Consumer Law, Intellectual Property, Privacy, Data Protection, Security and Dispute Resolution arise. Here also the Tier 2 Registrars will need to ensure that any Resellers are also bound, adhere and comply to all relevant legislation.

There is expected to be an onus upon the Registrants to undertake to maintain, correct and update information provided to the Tier 2 Registrar.
(See Registrants below at point 7)

4. **Authentication Agencies (AA)**

As the AA is responsible for the identification and validation of the information provided to the Tier 2 Registrars by the end user Registrant, in the situation where an AA is using a telecommunication service provider as the prime source for Authentication then the AA will be functioning as an interface between the Tier 2 Registrar and participating telecommunication service providers.

Also, if the AA is not implementing their own end user Registrant identification process then they must initially ensure that the Tier 2 Registrar has used due care in 'Identifying' the user before attempting to 'Validate' the user's right to use the telephone number. In this case, the AA will require commercial contracts with one, and usually more than one, Tier 2 Registrars.

The AA will also require commercial contracts with one or more participating telecommunications service provider(s) and will need to comply with data protection legislation and privacy legislation to both UKEPG (as part of accreditation of AA) and Tier 2 (as part of any commercial contracts).

5. **Telecommunication and other Electronic Communication Service Providers (TSPs)**

If a TSP participates then they will need to contract with one or more AA(s) to provide the interface that can be used by the AA to authenticate the user's right to register a telephone number from the TSP's assigned telephone number ranges.

6. **UK ENUM Application Providers (AP)**

Each application will have its own unique idiosyncrasies with regard to each application's legal perspective. However for illustration consider APs and those applications that may choose to support voice services for end user Registrants via ENUM. In this case the AP may wish to pay special attention to duties and obligations that apply and relate to Primary Line telephony services, whereby if an end user Registrant utilised their ENUM as their sole means of interoperating with the PSTN, then the Application service provider may also fulfil the role of Primary Line provider and therefore be required to support services in the event of power failure, and other services such as operator assistance and 999 emergency for which the AP cannot make charges.

UK ENUM Application Providers may also need to warrant or undertake that they shall comply with any legislative or regulatory requirements relating to consumer protection which may be applicable to the use of the Application / service and with any public policy related laws which may be applicable to the use of the service by third parties (such as privacy laws and laws relating to decency, libel or defamation), with respect **to the content** of communications transmitted using any service.

Consideration may also be required with regards to the Regulation of Investigatory Powers Act 2000.

7. **UK ENUM Registrants**

The general principles for consideration for statutory rights of Registrants must include, but are not limited to, the ENUM terms and conditions for end user participation (even in the event that such trial should cease or a Participant should leave the UK ENUM Trial).

These principles include such header subjects covered by:

- The Electronic Commerce (EC Directive) Regulations 2002
- The Consumer Protection (Distance Selling) Regulations 2000
- The Data Protection Act 1998 and Privacy laws
- The Competition Act 1998

Registrant and third party rights for the resolution of disputes
Specifically, with regards to the rights granted to Registrants to demand arbitration in the UK under the Communications Act 2003 (i.e. when any and all other complaint procedures fail or provide unsatisfactory resolution to the Registrant), an ENUM Registrant is entitled to alternative dispute resolution via the OTELO (The Office of Telecommunication Ombudsmen), or alternatively the CIA (Chartered Institute of Arbitrators). The costs of this must rest with the service

provider about whom the complaint is made or whose activity resulted in the dispute.

By way of example, and with regard to the protection of data, each Participant shall:

- ensure that in relation to personal data (as defined in the Data Protection Act 1998) provided by an End user Registrant to a Participant or passed by a Participant to another Participant adequate security measures must be taken to the standards set out in the legislation;
- not damage, alter, disclose, lose or destroy any personal data held by a Participant in respect of which that Participant or any of its affiliates is the data controller (as appropriate) for any reason up to 3 years from acquisition of that data except for the extent specifically instructed to do so in writing by the Registrant or Participant providing the personal data;
- not use any such Personal Data for any purpose other than one that has specifically been authorised, in writing, by the party providing such Personal Data.

Each Participant shall comply with all reasonable requests of the other Participant with regard to ensuring that the procedures operated by it and its affiliates to comply with their respective obligations from time to time (including without limitation with regard to collecting, holding, updating, using, disclosing and transferring the personal data (as imposed by such laws and regulations)).

Further considerations must also be given for an end user Registrant Agreement is that all ENUM Tier 1 database rights, including content shall remain under the jurisdiction and purview of the UKEPG (or any other body deemed responsible for ENUM policy within the UK).

Finally, it is also pertinent to mention the level of WHOIS support in relation to ENUM end user Registrants, insofar as WHOIS lookup functionality will at most only be partially enabled with regard to ENUM Domain Names (i.e. that WHOIS enablement should yield only the ENUM Registrar associated with an ENUM). This is due to the potential for look-up abuse and the privacy implications that arise thereafter. This specific issue may require a more vigorous investigation in due course.

8. **UK ENUM DNS providers**

As ENUM DNS providers will be responsible for the NAPTR records associated with individual ENUM registrations, and may be providing these DNS name server services to end user Registrants independently of the organisation(s) that were originally responsible for an ENUM's registration and may therefore have a separate billing relationship with a end user Registrant. It has been shown, separately within the UK ENUM Report, that ENUM DNS Providers may interoperate under various models that may co-exist during a production or commercial phase. These models detail a number of separate special scenarios that DNS providers will need to consider in depth. In summary thereof, ENUM DNS providers may require separate contracts with end user Registrants, Tier 2 Registrars as well as carrying obligations to the Tier 1 Registry. It is envisioned that NAPTR records could change regularly, and that the DNS providers could

also change just as frequently. All contractual relationships with ENUM DNS providers by other Participants must reflect this fluidity.

Annex H – Data Templates

The actual data formats used during the trial are listed in sections J.1 and J.2, whilst an example of enhanced EPP templates that have been designed and may be used in future trial activities is shown in J.3.

H.1 ENUM Authentication Application Data Format - Interface A & B

Fields 1.0 to 1.2 below contain information about the Registrar and will be passed across interface A. This information will be the same for each request. Fields 2.0 to 2.10 contains the Registrant information. Fields 3.0 to 3.4 is for use by the Authentication provider.

All of the fields labelled 1.x and 2.x are to be passed from the Registrar to the AA. The AA will return the fields labelled 2.x and 3.x to the Registrar. This information is passed across interface B.

	Field Name:	Type:	Data:	Example
1.0	registrar_ID:	[mandatory]	[single]	Reg1
1.1	password:	[mandatory]	[single]	Dummy
1.2	account:	[optional]	[single]	00001
2.0	title:	[optional]	[single]	Mr
2.1	name:	[optional]	[single]	John, Doe
2.2	organisation_name:	[mandatory]	[single]	Mycompany Ltd
2.3	street_address:	[mandatory]	[multiple]	10 Nowhere Road
2.4	town_city:	[mandatory]	[single]	Elsewhere
2.5	postcode:	[mandatory]	[single]	NVA L1D
2.6	first_enumber:	[mandatory]	[single]	+441234567890
2.7	last_enumber:	[optional]	[single]	+441234567890
2.8	telco_provider:	[mandatory]	[single]	Friendly Phones Ltd
2.9	telco_account_number:	[mandatory]	[single]	12345678
2.10	aob:	[optional]	[multiple]	
3.0	date_received:	[mandatory]	[single]	20030224
3.1	actioned_by:	[mandatory]	[single]	Joe Bloggs
3.2	status:	[mandatory]	[single]	Success
3.3	reference:	[mandatory]	[single]	00001
3.4	notes:	[optional]	[multiple]	

Note:

The data in fields labelled 1.x is intended to be replaced by a more secure authentication method such as SSL or private key authentication.

H.2 Interactions between the Registrar and Registry - Interface C

We list the information to be passed to the Registry by the Registrar pending successful authentication here. The method of submission in a commercial phase is a matter for the Registrar and may be email, XML (including EPP) or another method dependent on the Tier 1 bid process.

Throughout the trial so far email has been used as the interface for reasons of simplicity.

Authorization

- 0a. (N)ew (M)odify (R)enew:<N>
0b. User ID: [1] <Registrar ID>
0c. Password: [1] <for security - optional>
0d. Account: [1] <Staff identifier / customer Identification/ - optional>
1. Authentication Token: <supplied by Auth Agency to the Registrar>
2. Complete Domain Name: <looking like 9.8.7.6.5.4.3.2.1.4.4.e164.arpa>
2b. Last Domain Name: [2] <looking like 9.9.7.6.5.4.3.2.1.4.4.e164.arpa>
-

Person/Organization Using Domain Name

- 3a. Person/Organization Name:
3b. Street Address:
3c. Town/City:
3d. State:
3e. Post code:
3f. Country:
3j. Phone Number:
3k. Fax Number:
3l. E-Mailbox:
3m. Password:
-

Administrative Contact

- 4a. (I)ndividual or (R)ole:
4c. Name (Last , first):
4d. Organization Name:
4e. Street Address:
4f. Town/City:
4g. State:
4h. Postcode:
4i. Country:
4j. Phone Number:
4k. Fax Number:
4l. E-Mailbox:
4m. Password:
-

Technical Contact

- 5a. (I)ndividual or (R)ole:
5c. Name (Last , first):
5d. Organization Name:
5e. Street Address:
5f. Town/City:
5g. State:
5h. Postcode:
5i. Country:
5j. Phone Number:
5k. Fax Number:
5l. E-Mailbox:
5m. Password:
-

Name Server

- ns1b. Server Hostname:
ns1c. Server Net Address:
-

Name Server

- ns2b. Server Hostname:
ns2c. Server Net Address:
-

Optional Name Server

- ns3b. Optional Server Hostname:
ns3c. Optional Server Net Address:
-

Notes:

Items labelled 1 may be replaced by a more advanced security method as devised by the Registrar.

The pair of items labelled 2 denotes a 'range' of registrations that will be set up by the Registry using identical information - the supplied authentication token must match this.

H.3 Example EPP Interface

EPP interface is based upon current published EPP drafts. In addition to the published drafts, an extension is used to allow the passing of verification certificates to the Registry. In contrast with the published EPP ENUM document (draft-ietf-enum-epp-e164-02.txt), this schema does not include provision for specifying NAPTR records directly; a conforming implementation of this schema shall always perform delegations.

As shown in the examples below, verification certificates must be included within the <extension> section of <domain:create> requests.

The presence of the various contact types are a matter of Registry policy and therefore beyond the scope of this document. In these examples, the *admin* contact is always the Registrant, and there are separate contacts for *registrar* and *signing* (the party responsible for cryptographic keys and signing procedures). These contact types are given here for illustrative purposes only, and may not accurately reflect the operational policy of any active ENUM Registry.

At present, the <domain:transfer> command is not supported. Due to the nature of ENUM, it was felt that at the present time, the usefulness of supporting a transfer operation was far outweighed by the potential problems it could cause.

<domain:check> command

The <domain:check> command queries the server to determine whether a domain is available for registrations.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
  epp-1.0.xsd">
  <command>
    <check>
      <domain:check
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
        domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:name>5.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:name>6.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
      </domain:check>
    </check>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

<domain:check> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
  epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <resData>
      <domain:chkData
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
        domain-1.0.xsd">
        <domain:cd>
          <domain:name avail="1"></domain:name>
        </domain:cd>
        <domain:cd>
          <domain:name avail="0">5.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
          <domain:reason>In use</domain:reason>
        </domain:cd>
        <domain:cd>
          <domain:name avail="1">6.3.2.1.6.7.9.8.6.4.e164.arpa </domain:name>
        </domain:cd>
      </domain:chkData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54322-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

<domain:info> command

The <domain:info> command is similar in concept to the WHOIS service. A server response contains contact, nameserver and timestamp information for a domain.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <info>
      <domain:info
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
          <domain:name hosts="all">4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        </domain:info>
      </info>
      <clTRID>ABC-12345</clTRID>
    </command>
  </epp>
```

<domain:info> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <resData>
      <domain:infData
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:roid>D4672</domain:roid>
        <domain:status s="ok"/>
        <domain:registrant>C8013</domain:registrant>
        <domain:contact type="admin">C8013</domain:contact>
        <domain:contact type="tech">C8013</domain:contact>
        <domain:contact type="registrar">C7732</domain:contact>
        <domain:contact type="billing">C8013</domain:contact>
        <domain:contact type="signing">C8013</domain:contact>
        <domain:ns>
          <domain:hostObj>ns1.example.com</domain:hostObj>
          <domain:hostObj>ns1.example.net</domain:hostObj>
        </domain:ns>
        <domain:host>ns1.example.com</domain:host>
        <domain:host>ns2.example.com</domain:host>
        <domain:clID>ClientX</domain:clID>
        <domain:crID>ClientY</domain:crID>
        <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
        <domain:upID>ClientX</domain:upID>
        <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
      </domain:infData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54322-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

<domain:create> Command

The <domain:create> command is used to perform a registration.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <create>
      <domain:create
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:period unit="y">2</domain:period>
        <domain:ns>ns1.example.com</domain:ns>
        <domain:ns>ns2.example.com</domain:ns>
        <domain:registrant>C1234</domain:registrant>
        <domain:contact type="admin">C8013</domain:contact>
        <domain:contact type="tech">C8013</domain:contact>
        <domain:contact type="registrar">C7732</domain:contact>
        <domain:contact type="billing">C8013</domain:contact>
        <domain:contact type="signing">C8013</domain:contact>
        <domain:authInfo>
          <domain:pw>2fooBAR</domain:pw>
        </domain:authInfo>
      </domain:create>
    </create>
    <extension>
      <enum:create xmlns:enum="http://enum.org.uk/ns/enum-create">
        <enum:certificate>
          -----BEGIN VERIFICATION CERTIFICATE-----
          Version: ENUM Registry Platform

          hQIOAwkW87MhRC/IEAF/fGlarZFPIdOadgJ4B3ih9SsgtVZ15zduSWXpjYGyBLD
          XSjHTZfnerUPYPqKviK11iFQF89FvQa5ZbZntqTjIp6zmOtuiLzm01oR7cnz4reZ
          1KH9esP3UBw6ILXXbgTAYGXCzpg2lt/sHbDx3E3tkBFsdJLXZqd57grm+R0v9ui3
          EQpKvdxzalshqpdjSCoR5TQRbJcxSAP02VRxi3WamZTndiPraOqDFCp78uTR5QS
          RFJJQTwX7C7GKIzrHvi7MjM5GZy+XQZ9quHIM3CgHsbpRd9PsOtNDP7lu0jTN6xn
          YgQHckQ/JId65zEKXB/6/ghUwlT4cWkub65UTSB/KggA45NaTjupTBjotiSfyfWT
          NxTlOanAbISwYuUYK8NXmNtnUDkIhPP7Qevengpgf7VsQUwfDbHb83Fjw5SZ/kK4
          z3jIJIUDNh8XHHWpxHcjXhefa5CCtF/2Fg4xJdgifLFHe9oxycOUFdn57NCgrxNM
          uOSqtnyPfbzLBVV32F/zVgdebWb1L3CVHQZZ5DdY5RIkvA1YK6frgs+Xa+ohPyAQ
          MrswiajeiJXoskQlRe9A5bJSC0rOcllGkJ1xnwz22sKrsH+ut+PbOBX17XFobRwd
          +Oz7lgcOeP3igh+ic+dyJVfKkE2DZIxYQKARvX12LZYGD2sibw7adtN59fyfWEA0
          tdK3AUEtgK0muNRCTD1H76omitxI6wBwoZVqpKIFUMrT5mOw50lO5AKUT9Do28or
          iIBYsN7jHOnY985vEfldEg1Wp1OJ87syOB0Zjj92JNgDJ0f7EiDF51JXetQ1LyBH
          Zm8Jp1LCukOHeLPhybSgWVM/TlAotsLJqw7EH6gM2GUnb9aZP6rC8vRsLFmlz45z
          mycqUWCLP2asFdwLmXOknMG4PjU8ePSU0ZTkXLLCLxZ3gh0sv9s550U
          =oQms
          -----END VERIFICATION CERTIFICATE-----
        </enum:certificate>
      </enum:create>
    </extension>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

<domain:create> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <resData>
      <domain:creData
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:crDate>2003-04-03T22:00:00.0Z</domain:crDate>
        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
      </domain:creData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54321-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

<domain:renew> Command

<domain:renew> is used to perform a renewal (that is, extend the registration period).

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <renew>
      <domain:renew
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:curExpDate>2000-04-03</domain:curExpDate>
        <domain:period unit="y">5</domain:period>
      </domain:renew>
    </renew>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

<domain:renew> Response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <resData>
      <domain:renData
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
      </domain:renData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54322-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

<domain:update> Command

The <domain:update> command supports changing the nameserver information, and the technical, billing and signing contacts. The administrative contact (the Registrant) may not be changed using <domain:update>.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
  epp-1.0.xsd">
  <command>
    <update>
      <domain:update
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
        domain-1.0.xsd">
        <domain:name>4.3.2.1.6.7.9.8.6.4.e164.arpa</domain:name>
        <domain:add>
          <domain:ns>
            <domain:hostObj>ns2.example.com</domain:hostObj>
          </domain:ns>
        </domain:add>
        <domain:rem>
          <domain:ns>
            <domain:hostObj>ns1.example.com</domain:hostObj>
          </domain:ns>
        </domain:rem>
        </domain:update>
      </update>
      <clTRID>ABC-12345</clTRID>
    </command>
  </epp>
```

<domain:update> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
  epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54321-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

<contact:create> Command

<contact:create> is used to create a new contact object.

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <create>
      <contact:create
        xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:contact-1.0
          contact-1.0.xsd">
        <contact:type>role</contact:type>
        <contact:postalInfo type="int">
          <contact:name>John Smith</contact:name>
          <contact:org>Example Ltd.</contact:org>
          <contact:role>Telecommunications Officer</contact:role>
          <contact:addr>
            <contact:street>123 Example St.</contact:street>
            <contact:city>London</contact:city>
            <contact:pc>W1A 6WX</contact:pc>
            <contact:cc>GB</contact:cc>
          </contact:addr>
        </contact:postalInfo>
        <contact:voice x="1234">+447732712123</contact:voice>
        <contact:fax>+442089729721</contact:fax>
        <contact:email>john.smith@example.com</contact:email>
        <contact:authInfo>
          <contact:pw>2fooBAR</contact:pw>
        </contact:authInfo>
        </contact:create>
      </create>
      <clTRID>ABC-12345</clTRID>
    </command>
  </epp>

```

<contact:create> response:

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <resData>
      <contact:creData
        xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:contact-1.0
          contact-1.0.xsd">
        <contact:id>C8013</contact:id>
        <contact:crDate>1999-04-03T22:00:00.0Z</contact:crDate>
      </contact:creData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54321-XYZ</svTRID>
    </trID>
  </response>
</epp>

```

<contact:update> Command

<contact:update> is used to update contact information.

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <update>
      <contact:update
        xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:contact-1.0
          contact-1.0.xsd">
        <contact:id>C8013</contact:id>
        <contact:chg>
          <contact:voice>+447093327721</contact:voice>
          <contact:fax/>
          <contact:authInfo>
            <contact:pw>2fooBAR</contact:pw>
          </contact:authInfo>
        </contact:chg>
        </contact:update>
      </update>
      <clTRID>ABC-12345</clTRID>
    </command>
  </epp>
<contact:update> response:
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54321-XYZ</svTRID>
    </trID>
  </response>
</epp>

```

<contact:delete> Command

The <contact:delete> command is used to delete a contact object, and shall **not** succeed if the contact object is in use (that is, it is registered as a contact for any domain objects).

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <command>
    <delete>
      <contact:delete
        xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
        xsi:schemaLocation="urn:ietf:params:xml:ns:contact-1.0
          contact-1.0.xsd">
        <contact:id>C8013</contact:id>
      </contact:delete>
    </delete>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

<contact:delete> response:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
    epp-1.0.xsd">
  <response>
    <result code="1000">
      <msg>Command completed successfully</msg>
    </result>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>54321-XYZ</svTRID>
    </trID>
  </response>
</epp>
```

Annex I – Attacking ENUM Security

The ENUM system is being used to validate telephone numbers to Internet domains. As attackers will envisage ENUM to be of value for unlawful purposes, it will be attacked at registration, during usage and at renewal. The Registrant and Registrar, being most visible, are most vulnerable to attack.

Attacking ENUM means being able to register and use an Internet domain under *4.4.e164.arpa* without being traced to a real name, address or telephone number.

This annex highlights how UKETG envisages ENUM will be attacked and describes how an attacker can be tracked back to name and address.

1.1 Registering ENUMs

All areas of the ENUM registration are vulnerable to attack. An attacker can and will attempt to attack or spoof any part of the ENUM registration. This section shows how authentication, validation and accreditation prevent these attacks.

1.1.1 The Registrant

The Registrant can be anybody, from an attacker to a respectable person or trustworthy company. Companies are harder to fake than individuals, as they will generally register a block of numbers.

Company credentials are also harder to fake as they are listed publicly. Any attack from a company can be traced to a specific name and address, preventing this from happening.

The Registrant has to be validated by the Registrar. However, if the Registrant does not accept when the Registrar declines the Registrant for declining validation of the Registrant, the Registrant can request the Tier 1 Registry for confirmation as to why the Registrar has declined their validation

As stated in section 9, there are two steps in confirming an applicant's right to register a number: validation and identification. Here we try to avoid these two checks.

1.1.1.1 Faking validation details

When an applicant applies, they supply various customer details. Although the applicant can supply any details, they have to accept the required Terms and Conditions of usage and supply credit card details.

To fake the user details requires the applicant to register a telephone number that does not tally with their name and address. This, in general is not possible, as the Registrant has to have a valid account with a TSP.

1.1.1.2 Evading the Identification Check

Whilst this would seem to be a promising avenue for attack, it is not clear what Identification checks will be agreed for the commercial phase of ENUM deployment in the UK, and so whether or not an external attacker CAN avoid such checks.

1.1.2 The Registrar

Although the Registrar is visible, it cannot be attacked as it only collects data and passes it on to those required to receive it. Therefore, attackers cannot fool it.

1.1.3 The Authentication Agency

The AA is hard to locate by an attacker, as it exists “behind” the Registrar. The AA’s role is to provide an answer from either of TSP, DQ or paper documentation. The chances of incorrect results increase when the AA needs to do this at speed.

The customer providing supporting documentation in terms of paperwork or fax data can also attack the AA. An attacker can fake each of these, so obtaining an invalid ENUM address.

If the PIN Code random number generator is solvable, an attacker may discover the PIN generation scheme. From this, an attacker can discover how PINs are generated and collect ENUM addresses for other users.

1.1.3.1 Breaking the TSP Validation

The TSP provides a method to access customer data. As a user must have a valid account with the TSP to enter their account code, they will have previously registered with their TSP. The TSP will have taken the customer’s name and address and validated it according to their own validation checks (see section 11.3.3.1.1 for an example of registration with Vodafone). This, in practice, moves the threats and liabilities to the TSP. It moves the attack to “Can you fake a telephone number”? As no attack on this exists in public, this is a hard problem and implies that attackers are unlikely to attack this mechanism. The only way to fake TSP data is to set up your own registered TSP and offer telecoms services (including ENUM).

1.1.3.2 Breaking the DQ validation

The design of the authentication implies that DQ will only be used when the TSP refuses to take part, when they refuse to allow the ENUM system to authenticate to their customer data.

Assuming the AA works with a non-complying TSP, the authentication becomes a query to DQ. Querying DQ is the ability to check whether an applicant’s name and address tallies with their telephone number.

1.1.3.3 Invalid Phone / Fax Data

If DQ validation and the TSP query procedure fails, the AA has to authenticate using “supporting documentation”. As supporting documentation can be falsified in various ways, this is an area where the Registrant can provide false information, fooling the AA into registering an invalid ENUM address.

1.1.4 The DNS Provider

Even if an ENUM registration has been completed successfully for the person who has a right to such a registration, there remains a risk that the data “published” for this

registration may not be correct, either through errors in the provisioning process or through external attack.

1.1.4.1 DNS Poisoning

One effective method to accomplish this spread of disinformation is DNS poisoning (also called DNS spoofing). This tactic consists of convincing a name server that a domain has a different IP address.

1.1.4.2 DNS Hijacking

DNS hijacking or spoofing happens when a DNS server accepts and uses incorrect information from a host that has no authority to give that information. DNS spoofing actually “poisons” the cache by placing counterfeit data in the cache of the name server. These kinds of attacks can result in serious security problems for DNS servers that are vulnerable; for example, by causing users to be directed to incorrect Internet sites.

1.1.5 The Tier 1 Provider

Tier 1 is vulnerable to various problems:

- Handling high volumes of fake applications - to slow down the process of registering genuine applications
- Data mining/harvesting to grab customers of other Registrars
- Registrars who frustrate transfers away from them to another Registrar
- Maintaining correct info / new (email) address but not informing the Registry
- Malicious moving domains - employee leaves and presents valid docs only to establish it was an unauthorised transaction.

1.2 ENUM Address Usage

When an ENUM address is used, a recipient must be able to validate the user and check that the ENUM address is still valid.

An attacker will attack the address and its validation mechanism. The ENUM address of a user can be faked on usage only when the DNS address checked by the user can be faked. The ENUM address can only be faked in practice if an attack on the DNS can be constructed via DNS poisoning or DNS hijacking can be performed, If DNSSEC is used, ENUM cannot be faked and this problem is solved.

1.3 Renewing ENUM Addresses

When an ENUM registration is to be renewed, the Registrar and the Registrant (at least) will be informed. An attacker, on seeing that an ENUM address requires renewing, may pretend to be that user. As the user is already registered, it is possible that a Registrar shortcuts the AA and doesn't perform authentication checks in address creation.

Equally, a Registrant can claim that they have paid a Tier 1 provider for a renewal, but the Registrar hasn't received such payment.

1.4 Spoofing Attacks

The most obvious method to an observer of fooling ENUM registration is a spoofing attack, fooling the registration process into the idea that an element in the registration process can be faked.

Since all elements in the registration process have to adhere to stringent accreditation processes (see section 14), this is not possible. As long as these processes are maintained, spoofing all or part of the registration process cannot happen.

1.5 Special “Difficult” Numbers

There are telephone number ranges in the present UK telephone system that are registered for specific purposes. These include service numbers (e.g. 100 and 999) and premium rate numbers. These ranges are called “difficult” numbers, as they do not exist in standard TSP customer account records.

Difficult numbers are an easy target for attackers. As their registration is not public, TSPs will be reluctant to provide AAs with data based on their services. DQ services are also unlikely to display or provide information on such numbers. At present, these difficult numbers are an easy target for attackers to obtain an ENUM address under false pretences as they can only be validated via supporting documentation. Therefore, these numbers will require a specific mechanism that keeps data on these services private. This is an open question to be resolved.

1.6 Summary of Potential Attack Scenarios

In summary, the set of scenarios below describe the ways an attacker could break ENUM.

- Customer fakes user data
- Customer fakes supporting documentation for validation
- PIN Generation mechanism is broken or found to be predictable for Basic ENUM.
- DNS Poisoning / Hijacking
- DQ Lookup false positives
- Tier 1 Attacks
- Eavesdropping and altering data in transport
- Mobile ENUM-enabled device theft
- Implementation threats

Annex J – Trial Participants Remarks

This section is a retrospective view of the trial from the perspective of individual Trial Contributors. These remarks are the personal and company views and have not been endorsed by the whole UKETG but have been included in the report unedited.

J.1 Neustar, Inc.

NeuStar, Inc., the premier neutral third party provider of mission-critical database services to the telecommunications and Internet service industries has been involved in the ENUM trial since its inception. NeuStar has operated, in cooperation with ICB and Nominet, the Tier 1 Registry and contributed to the definition of technical and administrative specifications.

The UK trial has been one of the first ENUM national trials and has offered a great opportunity to gain valuable technical and operational experiences to pave the way to the introduction of ENUM commercial services in the UK. Validation and Authentication process, ENUM domain registration cycle, DNS infrastructure and operations are among the areas that have drawn clear benefits from the trial. Because of commercial and practical reasons, other areas such as user experience, business model and applications have been tested in a limited way during the trial.

To conclude NeuStar, Inc considers the trial a positive and useful exercise whose benefits will clearly emerge in the migration to the commercial phase.

J.2 Atlas Advanced Internet Solutions Ltd.

Atlas are an innovations based company and one of the UK's longest established Internet Service Providers. We have been involved in the ENUM trial since the start and have operated and contributed to the trial as the primary Registrar and as a DNS Provider for the duration.

Our work forms the basis for many of the recommendations for the commercial phase of the trials, including developing the UK's first working ENUM registration platform and recording the UK's first ENUM entry in February 2003, an important milestone for those involved in the project.

Our participation enabled the trial to test and refine models for ENUM DNS delegation and hosting, and enabled us to research and critically evaluate various models of end-user registration and authentication procedures, which have proven invaluable in arriving at the current recommended framework.

In summary, provided that the principles of competition and openness laid out in this report are adopted in the UK, ENUM is well positioned to become the leading unifying cross-platform communications enabler with great potential to revolutionise many diverse markets over the coming years.

Learn more at: <http://enum.atlas.net.uk> or about us at : <http://www.atlas.net.uk>