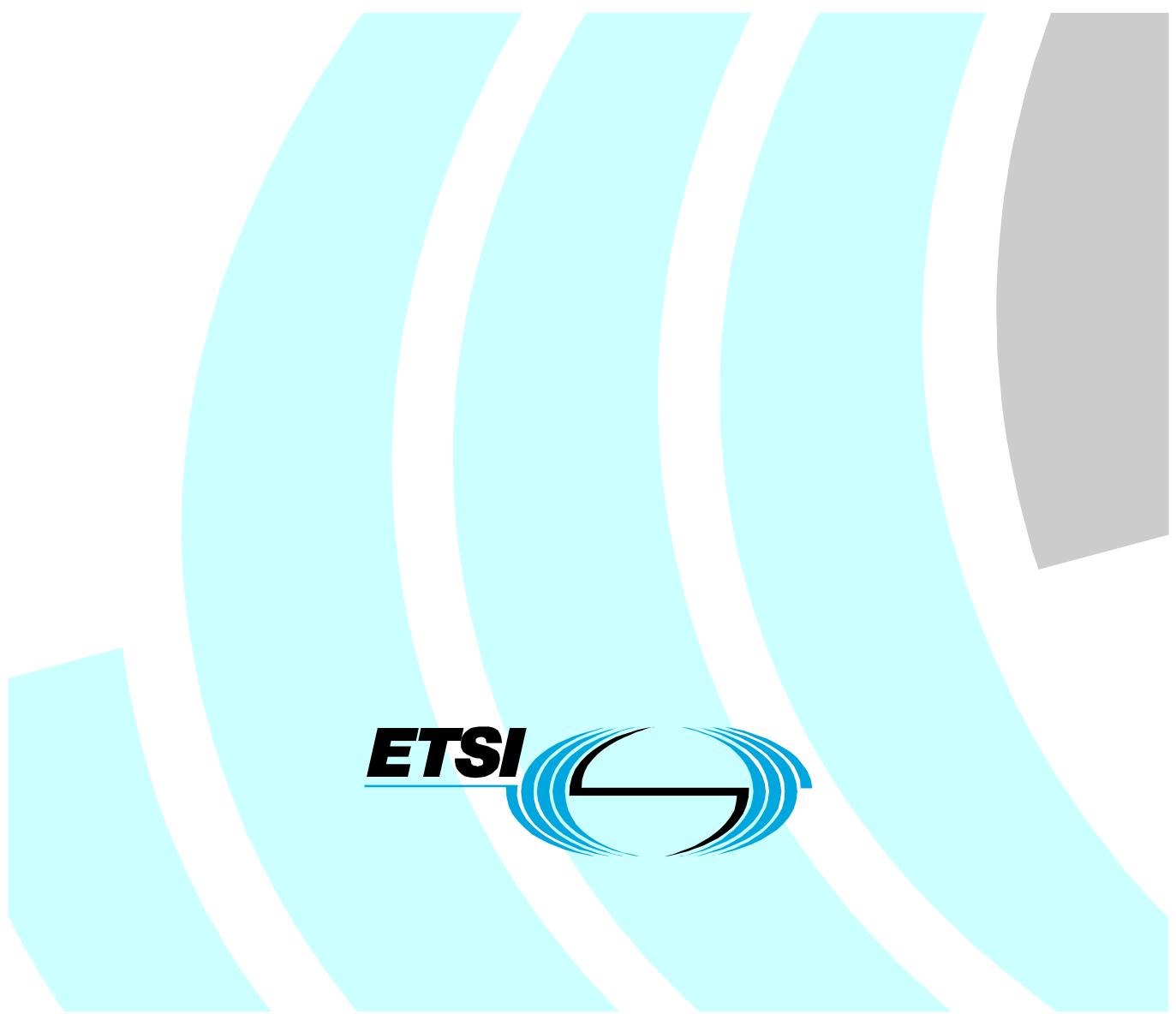# ETSI TS 102 051 V1.1.1 (2002-07)

Technical Specification

ENUM Administration in Europe

ETSI

Reference
DTS/SPAN-110106

Keywords
ENUM

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

1 Scope

The present document aims to assist European countries in the development of their national implementations of ENUM. The present document builds upon the concept of ENUM as specified in IETF RFC 2916 [1] limited to E.164. It introduces a set of basic principles that should be adhered to in order to maximize potential benefits from publicly available ENUM implementations within Europe. A functional architecture for ENUM administration is put forward and a number of options for provisioning flows are also proposed.

ENUM-like mechanisms can also be used for other identifiers or purposes such as private dialling plans, routeing, etc. These functions are out of the scope of the present document.

The description of applications that can be offered by using ENUM capabilities and the role to be performed by Application Service Providers are specified in TS 102 055 (see bibliography).

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

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

[2]   IETF RFC 1591: "Domain Name System Structure and Delegation".

[3]   ITU-T Recommendation E.105 (08/92): "International telephone service".

[4]   ITU-T Recommendation E.164 (05/97): "The international public telecommunication numbering plan".

[5]   ITU-T Recommendation E.191 (03/00): "B-ISDN addressing".

[6]   IETF RFC 954: "NICNAME/WHOIS".

3 Definitions and abbreviations

3.1 Definitions

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

accreditation: processes by which organizations are approved to act as the entities at the Tier 1 or Tier 2 levels

   NOTE: The nature of accreditation, indeed whether it applies at all, is a national matter.

Application Service Provider (ASP): entity that provides specific application(s) which may be linked to an E.164 number using ENUM e.g. email or voice messaging to the end user

assignment entity: entity (e.g. Telephony service provider or National Number Plan Administrator or his agent) responsible for the assignment of E.164 numbers to end users

designated manager or responsible administrative organization: entity, in any level of the ENUM-based architecture, which is responsible for a domain

NOTE: See clause 9.1 of the present document.

domain: set of host names within the DNS consisting of a single domain name and all the domain names below it

domain name: unique designator made up of symbols separated by dots

NOTE: The individual words or characters between the dots are called labels. The label furthest right represents the top level domain. The second most right represents the second level of domain, or "second level domain.

E.164: International Public Telecommunication Numbering Plan

NOTE: See ITU-T Recommendation E.164 [4].

E.164 Number: number taken from ITU-T Recommendation E.164

ENUM root: domain in which ENUM is hosted (according to IETF RFC 2916, this is e164.arpa)

ENUM domain name: domain name for an E.164 number

ENUM database: ENUM database is that part of the DNS below the ENUM root

ENUM end user: assignee of an E.164 number who has agreed to insert its E.164 number in the ENUM DNS-based architecture

ENUM registrar: entity that provides direct services to domain name registrants by processing name registrations

ENUM registrant: entity initiating the ENUM registration process (end user or agent)

ENUM subscriber: assignee of an E.164 number who has agreed to insert its E.164 number in the ENUM DNS-based architecture

ENUM Tier 0: level in the tiered architecture corresponding to the ENUM root, i.e. e164.arpa

NOTE: Records at this level contain pointers to Tier 1 for an E.164 Country Code or portion thereof.

ENUM Tier 1: level in the tiered architecture corresponding to the E.164 Country Code (CC), i.e. <CC>.e164.arpa

NOTE: Records at this level contain pointers to Tier 2 for an E.164 number.

ENUM Tier 2: level in the tiered architecture corresponding to the E.164 number, i.e., <N(S)N>.<CC>.e164.arpa

NOTE: Records at this level contain NAPTR records for an E.164 number.

ENUM Tier 2 Nameserver Provider: entity responsible for the servers within DNS that hold the NAPTR resource records

NOTE: In some other documents this entity is also referred to as the ENUM Tier 2 Registry or the ENUM Tier 2 provider.

National Number Plan Administrator (NNPA): entity responsible for the administration of a national numbering Plan that is part of the international E.164 numbering plan

number portability: ability of an end user to change location within a geographic area, between service providers or services, without changing their number

opt in: concept by which no action is taken unless with the explicit permission of the end user

telephony service provider: entity that provides the telephony service for which an E.164 number is assigned. In most cases the telephony service provider may act as the assignment entity

Uniform Resource Identifier (URI): compact string of characters for identifying an abstract or physical resource that is accessible via the Internet

Uniform Resource Locator (URL): refers to the subset of URI that identify resources via a representation of their primary access mechanism (e.g., their network "location"), rather than identifying the resource by name or by some other attribute(s) of that resource e.g. http://www.etsi.org or sip:user@etsi.org

validation entity: entity (e.g. Telephony service provider or National Number Plan Administrator or his agent) that validates the assignment of E.164 numbers to end users

WHOIS: database function that provides a look up capability of those on the Internet

3.2 Abbreviations

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

ASP	Application Service Provider
DNS	Domain Name System
DNSSEC	DNS SECurity extension
ENF	European Numbering Forum
IAB	Internet Architecture Board
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISOC	Internet Society
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LS	Location Server
NAPTR	Naming Authority PoinTeR
NNPA	National Number Plan Administrator
NRA	National Regulatory Authority
ONP	Open Network Provision
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
RFC	Request For Comment (IETF related standard)
RRs	(DNS) Resource Records
SCN	Switched Circuit Network
SIP	Session Initiation Protocol
TLD	Top Level Domain
TSP	Telephony Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

4 Background

ENUM is a mechanism (see note 1) that maps E.164 numbers to Internet domain names. Every E.164 number can potentially be used in ENUM. All portions of international or national numbering plans can be considered for inclusion, meaning that every E.164 number can potentially be used in ENUM. Much attention now surrounds ENUM as it facilitates interworking between telephony networks and applications that are reliant on the Internet. ENUM transforms, in real time, end users' E.164 numbers to other communications identities (see note 2) used for setting up connections. For example, this could be used for communications from the circuit switched telephone network (PSTN) to IP-based services and vice-versa. It can also assist end users who wish to be able to be reachable via several means of communication. ENUM capabilities are described in more detail in clause 5 of the present document.

NOTE 1: While ENUM strictly refers to the mechanism, in practical terms it is also used to refer to the wider implementation of ENUM, i.e. the populated database.

NOTE 2: Communications identity is a generic term including a name, a number or an address. For explanation of these three terms refer to ITU-T Recommendation E.191 [5]. This new English term is introduced in the present document in the absence of a suitable well-known generic English term covering both a name, a number and an address for use in electronic communications networks (e.g. PSTN, ISDN, PLMN, Internet and PSPDN).

Following completion of work on IETF RFC 2916 [1] by the IETF which introduced the ENUM mechanism, the focus of attention turned towards the ITU-T who began working with the ISOC/IAB to determine the Administrative requirements (see note 3).

NOTE 3: ITU-T Study Group 2 is developing a Recommendation, E.A-ENUM "Principles and procedures for the administration of E.164 geographic country codes for registration into the domain name system", and a Supplement entitled "Operational and administrative issues associated with national implementations of enum functions" which will offer guidance to national Administrations/NRA. Approval of the Recommendation is targeted for 12/2002.

Work is now under way in some European countries in order to understand the implications of ENUM and how it could be implemented. However this is occurring in a rather fragmented manner. Concerns over ENUM have also been expressed by a number of other parties, including the European Commission (see note 4) in the production of a paper that has been submitted to the ONP Committee. An experts group on Numbering, Naming and Addressing, created by the ONP committee, will also be considering whether any specific action relating to ENUM is required.

NOTE 4: The ONP expert group meet in December 2001 and in January 2002. Their results were provided to the ONP Committee. Then the ONP Committee made a contribution to the ITU-T SG2-meeting in May 2002 that was supported by the 15 MS in EU.

The numbering and addressing environment within Europe exhibits marked differences from that within the US and other parts of the world, so it is considered important that Europe looks closely at the administration issues that occur with ENUM. Efforts at drawing together a co-ordinated approach should not only result in a firm foundation for ENUM activities within the European environment, but should also assist in enhancing the competitive communications environment.

The present document is presented to assist with that task. It has been developed taking due account of the views and comments of other key European bodies, including the European Numbering Forum (ENF).

NOTE 5: In the present document, for consistency, the domain e164.arpa will be mentioned as the ENUM root domain of the ENUM DNS-based architecture. In the case that a different domain results from discussions between ISOC and the ITU the basic principles articulated in this paper will apply.

The single domain that is referred to throughout the present document as for the ENUM Tier 0 domain, is the e164.arpa domain. This domain is used only for convenience and given that domain is specified in IETF RFC 2916 [1], the IETF protocol in which ENUM is described. This should not assume that this domain will be the final choice which the ITU and relevant Internet governance bodies will agree on for the implementation of ENUM. The principles set in the present document are independent of the final choice of the ENUM Tier 0 domain and should not preclude a single authoritative solution at some future point in time, should this become agreed policy.

5   Description of ENUM

ITU-T Recommendation E.164 [4] describes the format and types of use of public telephone numbers (E.164 numbers). ENUM is a term that has been adopted to describe a Domain Name System (DNS) based mechanism which maps E.164 numbers into URIs.

Via ENUM, an E.164 number can be used as a single front-end to a variety of communication identities by which an end user can be contacted, including those used for phone, fax and email. This enables users who are the recipient of communications to indicate the means by which they wish to be contacted through a single number. The details of these communications identities can also be easily amended, added to, or updated without changing the number used for access.

The communications identities that can be accessed via a look-up of ENUM data may be associated with a wide range of applications, some of which are shown within figure 1.
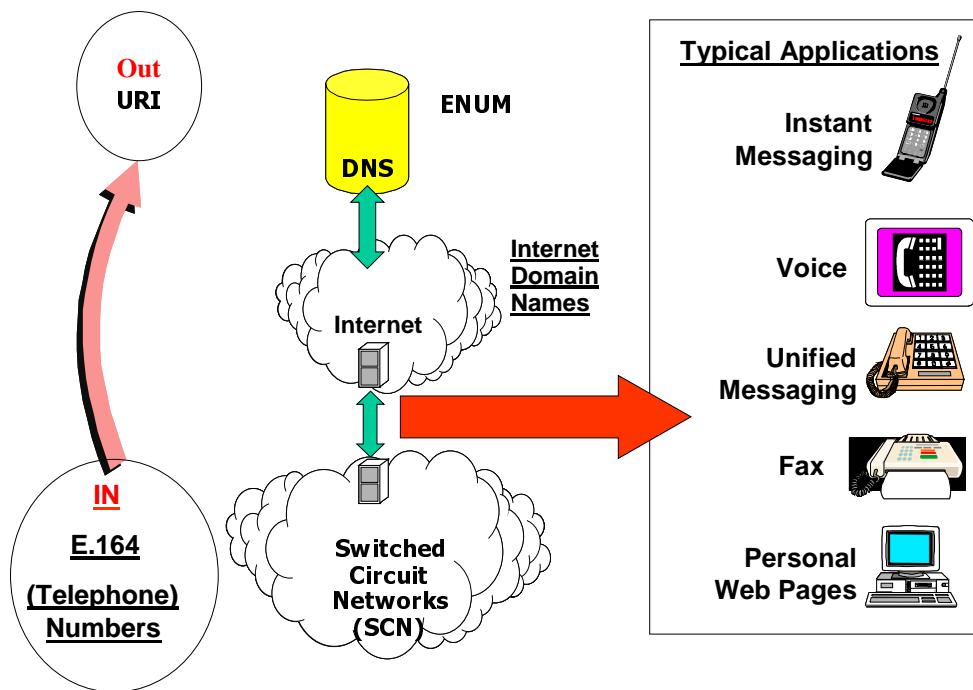
Figure 1: Typical applications enabled through ENUM

Using ENUM capabilities, providers of IP telephony services could legitimately originate IP telephony calls from an E.164 number or terminate IP telephony calls to an E.164 number that was assigned by the access network operator rather than by the IP telephony service provider.
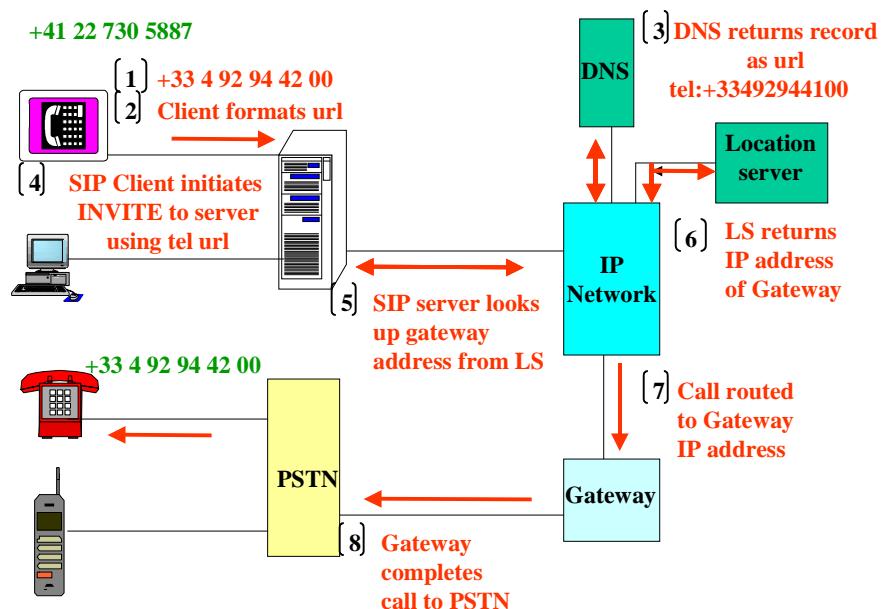
Figure 2: Typical call flows IP-PSTN

Figure 2 shows a typical call flow with a call originating on a SIP based network, in this example in Switzerland (+41 number), contacting a user on a SIP (IP based) network in France (+33 number).
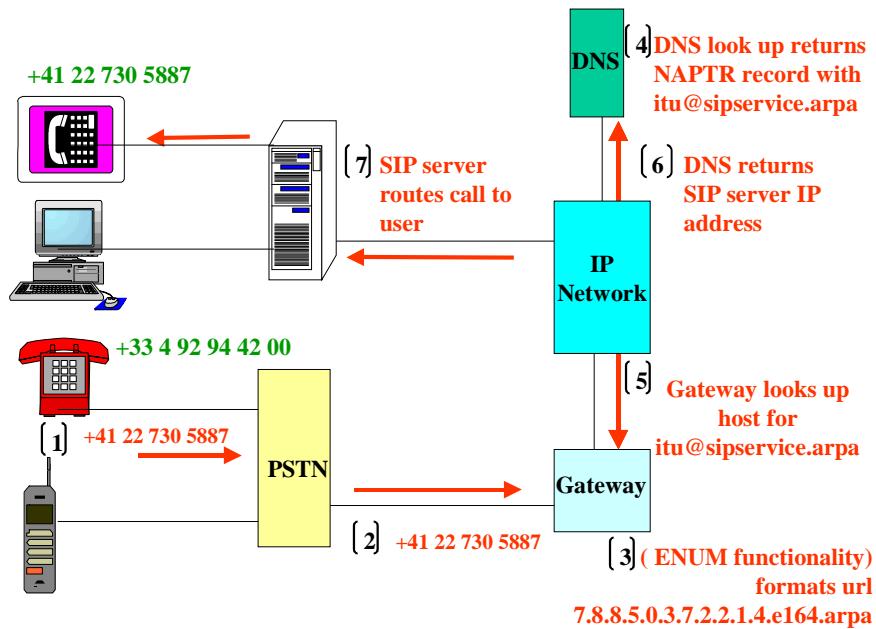
Figure 3: Typical call flows PSTN-IP

Figure 3 shows a typical call flow where a call originating on a on a circuit switched network in this case in France (+33 number), contacts a user on a SIP (IP based) network in Switzerland (+41 number).

It should be noted that ENUM can facilitate a wide range of different applications by providing access using an E.164 number, however ENUM itself does not provide these applications, merely a method that can facilitate access.

ENUM utilizes a mechanism developed by the Internet Engineering Task Force (IETF), specified in IETF RFC 2916 [1]. As stated previously ENUM resolution utilizes the DNS for resolution. The part of the DNS tree applicable to ENUM is shown in figure 4.
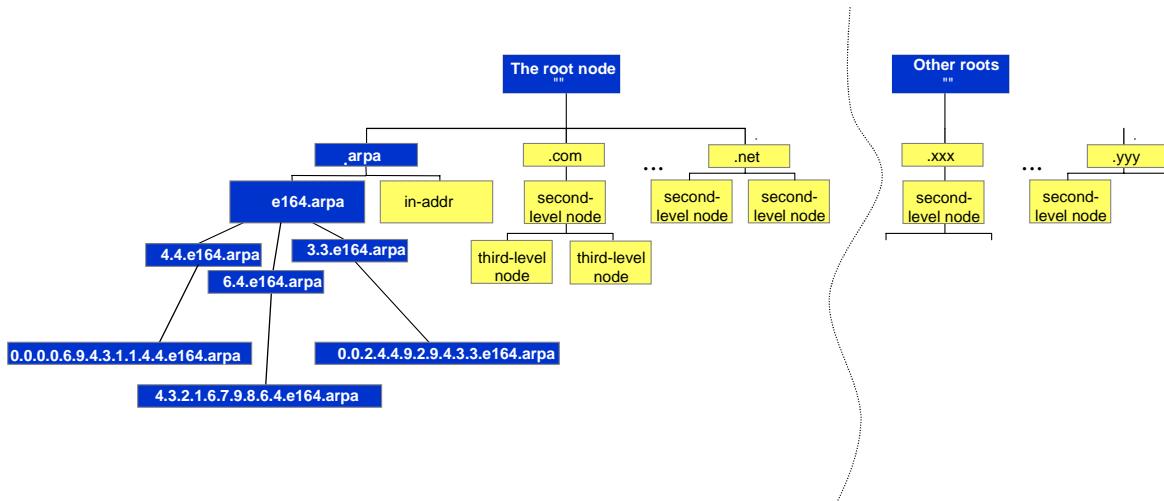
Figure 4: shows how ENUM fits into the DNS structure

The DNS forms a distributed database which holds information about Internet hosts. Each domain path spreads down from one 'root' domain at the highest level through its sub domains. In written form each sub domain is indicated by the insertion of a dot (.) within the written string. "Other roots" can be found in clause 6.3.3.

Second-level domains in other top level domains (e.g. enumworld.org and e164.com) are also possible and it must be recognized that multiple competitive ENUM DNS zones will be deployed. However, the approach in the present document focuses on a single domain as such an approach will provide a more authoritative, consistent and robust implementation of ENUM.

All types of assigned country codes: geographic country codes, Network country codes, global service country codes and Group of countries country codes could be inserted in the DNS.

To find the DNS names for a specific E.164 number, the following procedure is to be followed:

1) The E.164 number is written in its full form, including the country code.

2) All non-digit characters with the exception of the leading '+' are removed. The '+' is kept in stage 2 to flag that the number which the regular expression is operating on is an E.164 number.

3) All characters with the exception of the digits are removed.

4) Dots (".") are inserted between each digit.

5) The order of the digits is reversed.

6) The string ".e164.arpa" is appended to the end.

As an example E.164 number +33 492944200 is inserted in the DNS as the ENUM domain name 0.0.2.4.4.9.2.9.4.3.3.e164.arpa.

The ENUM domain name is resolved to other kinds of addresses (e.g. e-mail addresses, SIP URLs for "IP telephony", mobile telephone numbers, web addresses stored in special records, known as NAPTR records) which can thereby facilitate various communication solutions where telephone numbers are used as the only call identity.

These applications can all be provided using ENUM. To differentiate this use of ENUM from those that may use ENUM capabilities to facilitate routeing within a network operator domain, or alternatively within a private network environment the term "User ENUM" is sometimes used. The use of ENUM capabilities for Routeing within an Operators network is likewise sometimes referred to as "Infrastructure ENUM" (See TS 102 055 in bibliography).

6   Opportunities threats and risks

6.1   Possible opportunities from ENUM

ENUM is a key element for the convergence between IP based networks and networks offering telephony service such as PSTN, ISDN and GSM.

The introduction of ENUM may facilitate the development of IP telephony and other applications by enabling the recipients of communications to indicate what methods of communications are available for reaching them. The originator may be able to determine the most appropriate way to establish the communication.

Despite the staggering development of the Internet and the related addressing and naming schemes, it is worth remembering that E.164 is still the most used and widespread addressing and naming scheme and the only one supported by millions of devices currently in use. It is foreseeable that in the next few years both E.164 and Internet domain names will exist and increasingly inter-operate. What ENUM offers is a solution for interoperability between Internet domain names and any E.164 resource, establishing an environment for the creation of new services and applications. Any E.164 number can potentially be used in ENUM.

The possibility to associate a single E.164 number with a list of URIs allows an end user to have a single contact point (E.164 number) corresponding to a number of different services and applications such as voice, e-mail, fax, unified messaging, etc. The end user, by using the functionalities provided by ENUM, can customize his service profile and determine the preferred way to be contacted by the party initiating the communication.

It should be noted that the introduction of ENUM of itself does not require any change to the national numbering plans and will not imply any additional demand of E.164 number resources. However, new services and applications triggered by the availability of ENUM may generate demand for additional numbering resources.

ENUM is considered to be an enabler to the deployment of converged services and should therefore benefit Internet service providers, network operators, and end users. In order to maximize these benefits and avoid dangerous "side effects" such as incompatible implementations and leak of sensitive data it is crucial to develop an ENUM solution that addresses these issues and provides a pragmatic approach.

Operator population of ENUM for call routeing purposes may also provide additional functionality. TS 102 055 (see bibliography) describes how ENUM functionality could be used by operators for call routeing and examines the associated issues.

6.2   Possible threats from ENUM

It should be recognized that the potential of ENUM as a key enabler in the convergence between IP-based networks and more traditional telephony networks may also result in additional complexity in commercial relationships and regulation of the telecommunications sector. It is likely that both regulators and telephony service providers will face challenges from the quantum changes to the familiar telecommunications market structure and behaviour that ENUM may facilitate.

ENUM provides a significant risk for unscrupulous use of the information contained in NAPTR records. Any communication attempt to an E.164 number for which ENUM records exist will enable the requesting ENUM client application to access information on all of the service specific communication identifiers (telephone numbers, email addresses, Instant Messaging addresses, etc.) contained in that person's NAPTR record. This information could be used to determine the identity of the person associated with a randomly entered E.164 number (e.g. by looking at the name in their email address, or by looking at any other entry in their NAPTR record that gives a clue to their name).

This potential abuse of ENUM could be used to assist "identity theft" or to help organizations that wish to build lists of identities to use for the propagation of "Spam" communications across a wide range of different communications services (e.g. people who would previously contact people by working through lists of telephone numbers could now also generate lists of email addresses and instant messaging identifiers associated with those numbers).

Information contained in NAPTR records may reveal the types of communications applications and services that are used by an ENUM end user, and potentially also the providers of these applications and services. It is possible that this information could be used by third parties for commercial purposes; for example, to make offers to ENUM end user regarding applications and services that compete with those used by the subscriber, or to develop and sell market profiles showing the communications applications and services used by ENUM end users.

ENUM, like any system that maps multiple services to a single identifier (the E.164 number), can be vulnerable to multi-service Denial of Service (DoS) attacks. For example, anyone mounting a "flood attack" on the DNS NAPTR records can prevent the retrieval of any communication addresses from the NAPTR record. Such an attack would make it impossible for anyone querying the NAPTR record to get a response to their query. The result of such an attack could be that nobody would be able to communicate with the ENUM end user using any of their possible communication services, thus completely disabling the subscriber's incoming communications. Where the E.164 number associated with the NAPTR record is also provisioned in a PSTN network, it may still be possible to contact the person subjected to the DoS attack using that E.164 number in the PSTN network.

6.3   Possible risks from specific implementations of ENUM

Further threats may arise from particular implementations of ENUM that suffer from poor supervision or controls.

6.3.1   Integrity and security aspects

Two of the principal threats are:

- Passing off.

- Hijacking.

"Passing off" is where an entity represents itself as someone or something that it is not, usually to achieve a commercial advantage or for criminal purposes. In the context of ENUM, passing off could occur when an entity provisions another end user's E.164 numbers in the DNS by having their own details inserted in the NAPTR records corresponding to another person's or company's number.

Passing off is regarded as detrimental because it undermines the trust that individuals and organizations should have in communications using ENUM capabilities.

"Hijacking" is where a provider of communications applications and services is inserted in a communications path without an end user's permission. In the context of ENUM, hijacking could occur when:

- a provider of communications applications or services arranges for end users' E.164 numbers to be provisioned in the DNS without their consent; and

- communications using ENUM capabilities for these numbers are redirected via a network, application or service that end users have not chosen.

Hijacking regarded as detrimental because:

- it could allow a provider of communications applications or services to collect transit or other revenues improperly; and

- contradict an end user's decision regarding the carriage of its incoming communications.

These risks may arise from the following situation:

- that the contents of the IETF RFC 2916 [1] ENUM domain, together with those of various competing ENUM-like instantiations e.g. e164.com do not represent a consistent set of data; and

- that the contents of the IETF RFC 2916 [1] ENUM domain conflict with the assignments made in the E.164 numbering plan as maintained by the ITU and sub-delegations,

Both of these risks point to the need for adequate mechanisms to ensure that the request to provision a number in the DNS originates from the rightful assignee of the number. One possible method could involve authentication by the relevant Validation Entity. Whatever solution is developed, any effective method is likely to involve some degree of Validation. While these methods overcome the problem of "passing off", they may not completely solve the problem of "hijacking", as it is conceivably the Validation Entity which could be attempting to hijack the number. Similar issues occur in the case of amendment and withdrawal of a number. The challenge is to ensure that the processes meet requirements in order to maintain consistency between ENUM domain names and E.164 numbers, while not imposing an excessive administrative burden on any involved entities.

6.3.2 Abuse of market power

Additional risks arise due to the potential that ill-considered administration models could allow entities to abuse positions of significant market power. This chiefly arises around the Tier 1 Registry (see clause 8), which is a natural monopoly for a given CC or portion of a CC. Were a country to delegate rights to operation of this Registry without adequate controls, the Tier-1 Registry could potentially abuse its unique position, for example by charging a disproportionate fee for entering E.164 numbers into its database. Alternatively having more than one registry at the Tier-1 leads to many additional complications, including complex and difficult inter-working requirements. Measures to limit this potential abuse should be considered when national procedures are formulated.

6.3.3 Universal resolvability and uniqueness of data in DNS

The global, public DNS has a strictly hierarchical structure in which information for a given domain name is held in one, and not more than one, location in the DNS tree. It can be expected that multiple parallel ENUM-like zones will be deployed under other TLDs. This presents a fundamental risk to ENUM, as it undermines the principle of a unique location in the DNS tree for the data associated with a given E.164 number.

With parallel ENUM-like zones, there is no longer a unique location in the DNS tree for the data to be associated with a given E.164 number. Moreover, different data may exist for a given number in different zones. Note that in practice, the hierarchical structures of both DNS and the E.164 numbering plan have not inhibited competition in Internet and communication services: the hierarchical structure brings the stability in naming needed by all market parties.

The same fundamental risk would appear if ENUM-like zones were created under what is known as 'alternative roots' (domain name trees which are not under the purview of ICANN/IANA). These roots are a serious threat to the universal resolvability of the DNS - the basic functionality of the Internet that guarantees consistent and reliable name resolution - because a given name may be resolvable only in a particular root.

6.4   Other risks

It is possible that control of the domain in which ENUM is hosted by managers of a single country or region could provide that country or region with undue influence over the operations of converged Internet-telephony networks. Similarly, if the location of Domain Name Servers upon which the ENUM mechanism depends lies predominantly in a single country or region this may result in communications within Europe or between Europe and other regions being unduly reliant on infrastructure outside Europe. Any resolution of this issue is outside the scope of the present document.

7   Principles for ENUM implementation within Europe

ENUM shall conform to relevant regional directives, national laws and telecommunications specific regulations where appropriate. Specific principles that shall be applied to ENUM are set out in the following clauses.

7.1   Basic principles

The following basic principles shall be considered as key requirements when ENUM implementation administration aspects are considered.

- The ENUM end user must be the assignee of an E.164 number to ensure the integrity of the E.164 numbering plan.

- The integrity of the ENUM data shall not be compromised.

- Administration requirements must take due account of the different number types and methods of management of the E.164 Numbering Plan.

- The tenets of relevant ITU-T Recommendations, and IETF technical specifications should be adhered to.

- A competitive environment within Europe and compliance with all aspects of competition law shall be facilitated.

- A stable and secure environment which does not jeopardize the stability and functionality of the Internet and telecommunication networks (e.g. PSTN, ISDN and PLMN) shall be provided. The use of DNSSEC to provide additional security should be considered.

- There must be full conformity with regional and national data protection and privacy laws for all data within ENUM.

- Handling of numbers in ENUM shall occur in a manner that is in full accordance with relevant national regulatory requirements.

- Existing network functions such as Number Portability which are often provided as national implementations, must not be compromised.

- The Opt-in principle shall apply for end users to participate in ENUM (see clause 7.2).

- ENUM should not be inhibited if the relevant assignment entities choose not to participate.

7.2   Opt-in principle for the individual E.164 number holder

The assignee of a number must make an explicit request to participate in ENUM before the ENUM domain corresponding to that E.164 number can be registered and any NAPTR records for the number can be populated. This is important since records in ENUM are publicly accessible via DNS query. The opt-in process should be designed to ensure the following:

- Users can control privacy and integrity of their information.

- The default condition is not to include NAPTR record information.

- Any request for inclusion must be authenticated as being from the assignee of the E.164 number.

- Inclusion of NAPTR record information must be reversible, allowing the party to remove the data from the DNS in a timely fashion.

- Users are made aware in an appropriate and clear manner that information regarding their communications identities that is maintained in NAPTR records cannot be protected anywhere in the world.

ENUM entries for the sole use for network operators not complying to the opt-in principle must therefore be entered either in ENUM-like trees which are not available via the public DNS tree, or populated in a public ENUM tree parallel to e164.arpa, provided that no personal data is used (see TS 102 055 in Bibliography).

7.3   Principle for calling users and communications providers

The default service delivered to the calling user who enters an E.164 number is the existing telephony service according to ITU-T recommendation E.105 [3] without ENUM involvement. This implies that:

- No originating party (e.g., a calling user or a communications provider) is obligated to perform an ENUM query to complete a telephone call to an E.164 number.

- A party making an ENUM query, whether a calling user or communication provider, is not obligated to use any of the services in the NAPTR records returned.

- The specified number should be appropriately terminated for calls that originate on the PSTN/ISDN/PLMN. This termination could also be an announcement.

8   Functional model

Figure 5 depicts the ENUM reference model and the entities performing the different functions.

The ENUM functional and administrative model is based on the separation into three distinct levels: Tier 0, Tier 1 and Tier 2.

Different functions are performed at the three levels.

The main functions performed at Tier 0 level are the administration and technical management of ENUM domain. These functions are implemented by the Tier 0 registry that is a single international registry containing pointers to the Tier 1 registries.

The main functions performed at the Tier 1 level are management and operation of the ENUM domain corresponding to an E.164 country-code in the country or area identified by that given country code. These functions are implemented by the ENUM Tier 1 registry that is a national registry containing pointers to the ENUM Tier 2 Nameserver Providers.

The main functions performed at the Tier 2 level are the commercial provision of the ENUM functions. These functions are implemented by the ENUM Tier 2 Nameserver Provider and ENUM registrar which can be carried out by the same or separate entities.

The introduction of a tiered architecture ensures that two important goals are achieved. The first one is that the ENUM architecture follows the DNS hierarchy based on delegation as a mechanism to decentralize the control and provide the required level of scalability and security.

The second one is that competition and customer choice are properly introduced at the level where ENUM-based services are commercially offered (Tier 2) without interfering with administration and registry functions performed at the Tier 0 and Tier 1 levels.
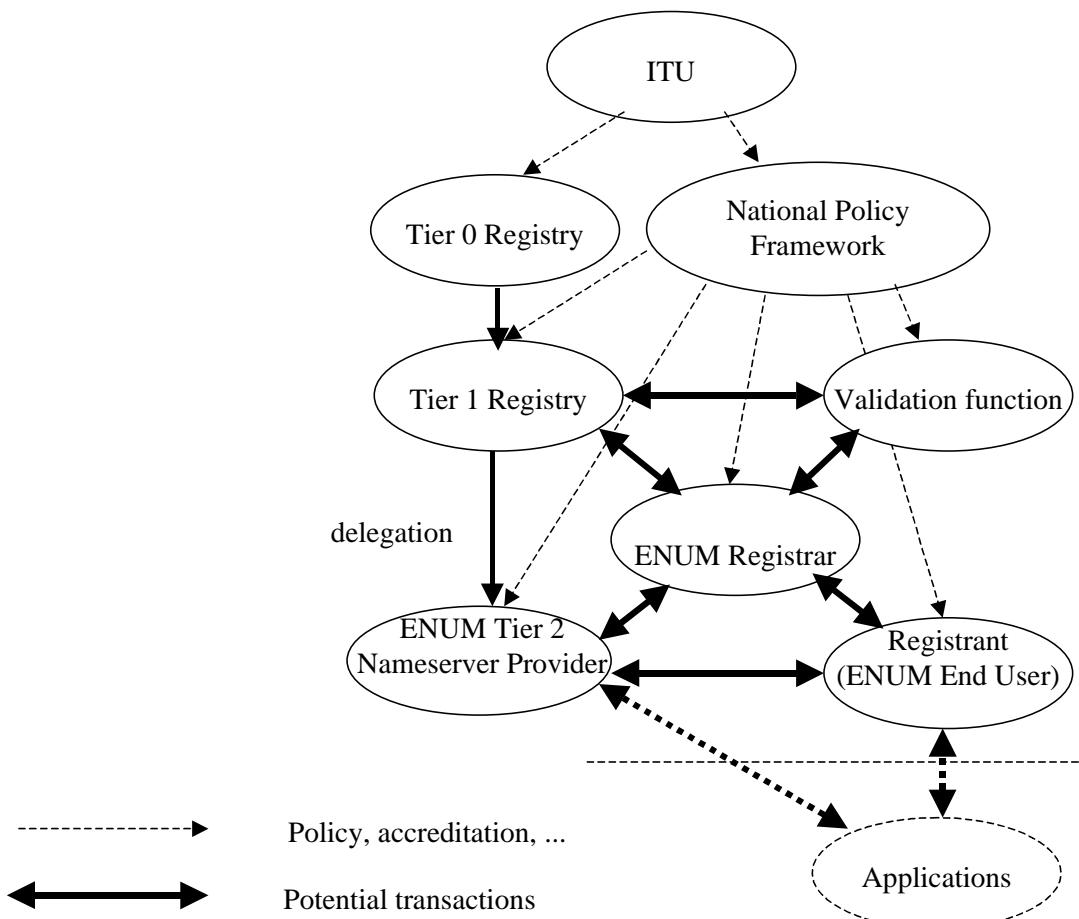
Figure 5

9   DNS responsibilities

This clause describes responsibilities for different domains in the Domain Name System (DNS) that are specific for ENUM implementations according to IETF RFC 2916 [1]. At the top of the domain name tree is the root domain ".". Further down in the domain name tree there are several branches for different domains, both geographic and generic. The DNS model (entities, their role and responsibilities) can be applied to ENUM DNS-based architecture only to some extent as more entities are involved in the management of ENUM domain names than in gTLD or ccTLD domain names.

A table attached to the present document as annex B summarizes the responsibilities between the different functions for the root domain and domains for ENUM in the DNS.

9.1   Administrative responsibility for a domain

In the DNS there is always an entity that is responsible for a domain. This role is referred to in the present document as the Responsible Administrative Organization for the Domain and in clause 3 of IETF RFC 1591 [2] as the designated manager (also designated authority - see note - - is used in the RFC). In addition, clause 3.1 of IETF RFC 1591 [2] requires an *Administrative Contact* and a *Technical Contact* for a domain. The Responsible Administrative Organization for the domain can either act itself as the Technical Contact for the domain, i.e. act as the *Registry*, or designate some other organization act as the Registry via a contract or agreement. IETF RFC 1591 [2] also specifies the functions of *billing contact* and *domain holder*; these are normally included within the role of the Responsible Administrative Organization for the Domain, but could be performed by other entities.

> NOTE: In other documents this role is also called: *administrator, domain administrator* or *TLD manager*.

9.2   Registry for a domain

The Technical Contact for a domain acts as the Registry and is the entity that has the register (original database) listing the Internet domain names that are registered in the domain. The Technical Contact is also responsible for operating the name server corresponding to the domain, i.e. this entity acts as the DNS operator. A Registry can either act as the DNS operator by itself or let some other entity be the DNS operator via contact or agreement. Production of the zone file for a domain is part of the responsibility of a Registry.

9.3   Registrar for a domain

The Registrar is the entity that handles applications for Internet domain names in a domain. The Registrar acts as an agent between the domain name holder (Registrant) and the Registry.

10   General administrative and operating assumptions and requirements

The ITU Member State has the authority for its part of the E.164 Numbering plan independent of ENUM i.e. the appropriate E.164 Country Code. For ENUM the ITU Member State may also assume the authority for the ENUM domain name corresponding to the E.164 Country Code assigned to the state. This responsibility is included in the role as being the ENUM Tier 1 Manager, i.e. the Member State will be responsible for managing the domain as being the domain name holder. This responsibility can then be legally delegated to the relevant NRA/NNPA or another suitable organization which will be noted as the Administrative Contact according to IETF RFC 1591 [2]. In order to achieve the delegation from Tier 0 to Tier 1, the Manager shall designate a suitably qualified organization as the responsible technical organization for the domain, i.e. the entity that will act as the ENUM Tier 1 Registry. The Member State will be and remain the responsible administrative organization for the portion of the ENUM DNS structure corresponding to the portion of the E.164 numbering plan under its control. (See annex B.)

> NOTE 1:   Responsibility for an ITU Member State's part of the E.164 numbering plan may, in the case of an integrated numbering plan, apply only to one part of a country code.

> NOTE 2:   Multiple Tier 1 Registries controlling different portions of a national number scheme are possible.

The decision to participate in ENUM with the inclusion of E.164 national numbering resources in the DNS is a national matter. Each European country is then responsible to decide whether its national E.164 numbers are allowed to be used in the ENUM context and how the administrative and operational process is organized. Therefore implementations within Europe may vary from country to country but should fit within the general framework described in the present document. Although ENUM Tier 1 and Tier 2 implementations are national matter in order to provide some support to the decisions of the countries and develop European guidelines for the definition of the administrative process the following proposals are made.

10.1   ENUM Tier 1 manager assumptions

- As a national matter the ITU Member State makes the decision to participate (opt-in) in ENUM.

- The ITU member state can legally delegate the responsibility to act as the Manager to the relevant NRA, NNPA (if separated from the NRA) or other suitable organization who may then be noted as the Administrative Contact according to IETF RFC 1591 [2].

- The ENUM Tier 1 Manager may decide to designate who will act as the ENUM Tier 1 Registry.

- The ENUM Tier 1 Manager will set up procedures to follow by the ENUM Tier 1 Registry when delegating domains to ENUM Tier 2 Nameserver Providers.

10.2   ENUM Tier 1 registry assumptions

- Rules or guidance (e.g. accreditation) procedures and requirements that address the following criteria shall exist to ensure that Tier 1 Registries achieve high quality of service and meet consumer safeguards:

  - the operation of the Registry database is accurate, robust and resilient, and is in accordance with specified service performance and availability standards;

  - zone files are generated;

  - both a primary authoritative name server and a secondary name server are provided in accordance with IETF standards for the DNS and with specified service performance and availability standards.

- Registry systems are implemented in accordance with appropriate information security management standards;

  - a business continuity plan for the Registry system is implemented that specifies the processes to be undertaken to ensure the continued operation of the Registry in the event of a disaster;

  - customer service is provided to all Registrars, and Registrars are able to enter and update the records in the Registry in accordance with the relevant IETF protocols;

  - all Registrars are dealt with in a timely manner and on an equitable basis;

  - final checks on domain name registrations are performed to maintain the integrity and stability of the Registry database;

  - the Responsible Administrative Organization for the Domain is advised of the status of the domain; and

  - specified accountability procedures are followed.

- In the event that the Registry goes out of business, Registrants will maintain the rights to have use of domain names and NAPTR records corresponding to their E.164 numbers and steps should be taken to minimize the impact on the ENUM operations e.g. data escrow.

- The Registry may decide to outsource some of its functions e.g. DNS operations to one or more neutral third parties.

- Consideration should be given to the provision of a WHOIS capability that takes due account of any data privacy requirements. The provision remains a national matter.

10.3   ENUM Tier 2 Nameserver Provider assumptions

- There may be a number of ENUM Tier 2 Nameserver Providers competing with each other.

- Without limiting the range of options the ENUM Tier 2 Nameserver Provider could be a telecommunication network operator, service provider, or third party offering services associated with an E.164 number to be inserted in the DNS or the ENUM end users themselves.

- Rules or guidance (e.g. accreditation) procedures and requirements that address criteria such as the following shall exist to ensure that ENUM Tier 2 Nameserver Providers achieve high quality of service and meet consumer safeguards. Care must be taken to ensure that these do not impose onerous overheads which would provide barriers to nameserver operations:

  - the operation of the Nameserver is accurate, robust and resilient, and is in accordance with specified service performance and availability standards;

  - zone files are generated;

  - both a primary authoritative name server and a secondary name server are provided in accordance with IETF standards for the DNS and with specified service performance and availability standards.

- Nameserver systems are implemented in accordance with appropriate information security management standards:

  - a business continuity plan for the Nameserver system is implemented that specifies the processes to be undertaken to ensure the continued operation of the Nameserver in the event of a disaster;

  - all NAPTR Resource Records of a given E.164 number are kept by a selected single ENUM Tier 2 Nameserver Provider.

  - all parties are dealt with in a timely manner and on an equitable basis and the records in the Nameserver are updated in accordance with the relevant IETF protocols;

  - final checks are performed to maintain the integrity and stability of the Nameserver.

- Procedures that permit Registrants to change the Nameserver Provider without interruption in use of the domain name and NAPTR records corresponding to their E.164 number are established.

- The ENUM Tier 2 Nameserver Provider may decide to outsource some of its functions e.g. DNS operations to one or more neutral third parties.

10.4   ENUM Registrar assumptions

- There may be a number of Registrars competing with each other.

- Without limiting the range of options, Registrars may include telecommunication network operators, service providers or third parties offering services associated with an E.164 number to be inserted in the DNS.

- Rules or guidance (e.g. accreditation) procedures and requirements that address criteria such as the following shall exist to promote high quality of service among Registrars and safeguard consumer interests:

  - secure, authenticated access to the Tier 1 Registry and ENUM Tier 2 Nameserver Provider(s) is implemented;

  - robust and scalable operations are established;

  - prompt handling of Registrants' requests for changes in domain name registration and NAPTR record data is provided;

  - reliable and readily usable backup and archival of all Registrant and registration data is implemented;

  - Registrar systems are implemented in accordance with relevant information security management standards;

  - in the event that the Registrar goes out of business, Registrants will continue to have use of domain names and NAPTR records corresponding to their E.164 numbers and operation of the Internet will not be adversely affected;

  - a Registrant grievance resolution process is implemented;

  - all terms and conditions associated with registration of domain name names and creation of NAPTR records corresponding to E.164 numbers, including price and billing information, are fully disclosed to Registrants;

- procedures that permit Registrants to change Registrar without interruption in use of the domain name and NAPTR records corresponding to their E.164 number are established;

- all rights to ownership or exclusive use of domain names corresponding to E.164 numbers are disclaimed;

- minimize the possibility for or occurrence of fraudulent transfer of domain names corresponding to E.164 numbers; and

- minimize the possibility for or occurrence of retention by the Registrar of domain names corresponding to E.164 numbers following the expiration or cancellation of registration.

10.5   Application Service Provider assumptions

In the functional model, the Application Services Providers (ASPs) provide the services, to which the NAPTR in the ENUM Tier 2 Nameserver Provider are pointing. This implies, that the end user has subscribed to at least one service with a given ASP.

Applications are outside the scope of the present document and so no assumptions are made about the ASP.

10.6   Registrant assumptions

- The ENUM user shall be able to choose the ENUM Tier 2 Nameserver Provider and ENUM Registrar he wants to use for a given E.164 number.

- The ENUM user may decide to delegate the provisioning and management of NAPTR RRs to a third party e.g. ASP.

- The choice of Application Service Provider for a given ENUM-based application shall not be constrained by the choice of ENUM Registrar or ENUM Tier 2 Nameserver Provider.

- The ENUM user has the right to decide whether his assigned E.164 number is inserted or withdrawn within the ENUM database.

- The ENUM user has full control over the provision and content of the NAPTR Resource Records in the ENUM Tier 2 nameserver.

10.7   Validation assumptions

The validation of the relation between an E.164 number and the telephony subscriber as well as the status of an E.164 number (still in service or not) is crucial in ENUM. The entity responsible for the validation shall verify that the ENUM Registrant is complying with all national rules given by the regulatory framework for this purpose.

- The registrant shall be the assignee of the specified E.164 number.

- The specified number shall be part of a number range allowed to be entered into ENUM.

- The specified number should be appropriately terminated for calls that originate on the PSTN/ISDN/PLMN. This termination could also be an announcement.

10.8   Removal assumption

- An E.164 number shall be removed from ENUM Tier 1 Registry and ENUM Tier 2 Nameserver provider when the Registrant requests its removal, when the number is withdrawn, or when the ENUM end user returns the number.

10.9   Other assumptions

- The fact that an E.164 number has been ported must not prevent the insertion of that number in ENUM.

- Controls must be established to prohibit malicious redirection of calls and avoidance of fraud.

- Measures need to be defined to accommodate unlisted (ex-directory) numbers within ENUM.

11   Operational and administrative processes

This clause describes some of the main processes needed in ENUM implementation: insertion, amendment, and removal. Other processes will be needed. It is expected that these processes are similar to the ones shown here.

At each level of the functional architecture, operational and administrative requirements need to be established.

11.1   Processes for the provision of records in ENUM database at the Tier 0 level

This clause is subject to agreements made between the ISOC and the ITU-T and is outside the scope of the present document.

11.2   Processes for the provision of records in the databases at the Tier 1 and Tier 2 levels

This clause describes the processes for registration and removal of E.164 numbers in the Tier 1 and Tier 2 databases and the insertion, amendment and removal of NAPTR records in, the ENUM Tier 2 Nameserver Provider.

11.2.1   Registration of an E.164 number in the ENUM database

This clause describes the process for registration of a new ENUM domain name in the ENUM Tier 2 Nameserver Provider and the delegation of the related zone in the Tier 1 Registry. The process is based on the assumption that the request of registration is initiated by the end user to which the E.164 number has been assigned or by a third party (agent) operating on behalf of the end user after its authorization. In the following the entity initiating the registration process (end user or agent) is referred to as the ENUM Registrant.
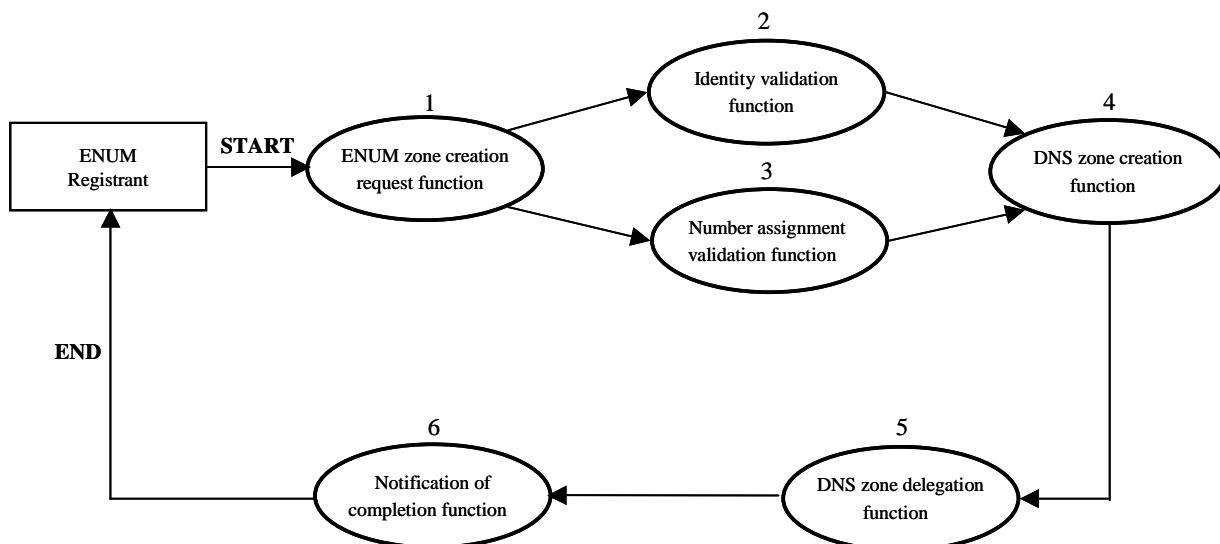
Figure 6: Functional model for Registration

Figure 6 represents a functional model and should not be considered as a business model as variants may exist.

As shown in figure 6, the following process takes place for the registration and provision of NAPTR records:

1) The **ENUM zone creation request** step involves receiving requests from an ENUM Registrant to create a DNS zone for his E.164 number.

2) The **identity validation** step involves confirming the identity of the ENUM Registrant and their authority to act on behalf of an end user.

3) The **number assignment validation** step involves confirming the assignment of the E.164 number to the ENUM end user.

4) **The DNS zone creation** step involves creation of a zone in the ENUM Tier 2 Nameserver Provider.

5) The **DNS zone delegation** step involves delegating DNS authority to the new zone by inserting the appropriate pointers in the Tier 1 Registry to the ENUM Tier 2 Nameserver Provider selected by the end user.

6) The **notification of completion** step involves informing the ENUM Registrant that the registration process has been successfully completed.

11.2.2 Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database

This clause describes the process for amendment of NAPTR Resource Records in the Tier 2 database. This could take the form of the creation, modification or deletion of a NAPTR or group of NAPTR records related to a specific E.164 number. A request for amendment is initiated by the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant).

Figure 7: Functional model for amendment of NAPTR Resource Records in Tier 2 database

Figure 7 represents a functional model and should not be considered as a business model as variants may exist.

The following process takes place for the amendment of NAPTR Resource Records in the Tier 2 database:

1) The **NAPTR Resource Record request acceptance** step involves receiving requests from an ENUM Registrant to create, modify or delete a NAPTR Resource Record corresponding to the ENUM end user's E.164 number.

2) The **identity validation** step involves confirming:

- the identity of an ENUM Registrant who is the ENUM end user; or

- the identity of an ENUM Registrant who is not the ENUM end user and its authority to make a request on behalf of the ENUM end user.

3) The **DNS zone update** step involves updating ENUM service details corresponding to the ENUM end user's E.164 number in the DNS in the required format.

4) The **completion notification** step involves informing the ENUM Registrant that the amendment process has been successfully completed.

11.2.3   Processes for removal of E.164 numbers from ENUM databases

This clause describes the process for removal of E.164 numbers and NAPTR Resource Records from ENUM databases. The process is based on the assumption that an ENUM end user should have information corresponding to its E.164 number in ENUM databases until:

- it no longer requires the services that are reliant on ENUM;

- it otherwise relinquishes the number or the number is withdrawn.

In the event of relinquishment or withdrawal of the number, it is important for NAPTR Resource Records corresponding to the number to be removed before any conflict is generated by use of the number by a new end user. In the case that the ENUM end user requires the removal of information relating to its E.164 number from ENUM databases, the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant) initiates the removal request. In the case that the ENUM end user relinquishes the number or the number is withdrawn, it may be appropriate to allow the Assignment Entity to initiate the request to remove information relating to the E.164 number from ENUM databases, or to periodically verify that ENUM data corresponding to an end user's E.164 number should continue to be maintained.
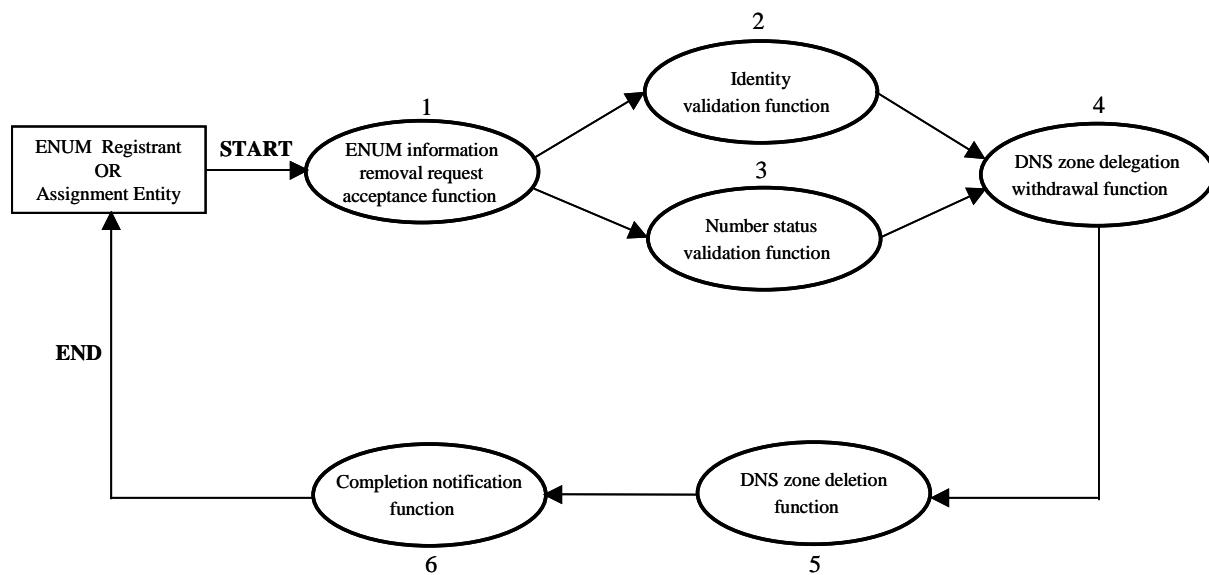
Figure 8: Functional model for removal of E.164 numbers from ENUM databases
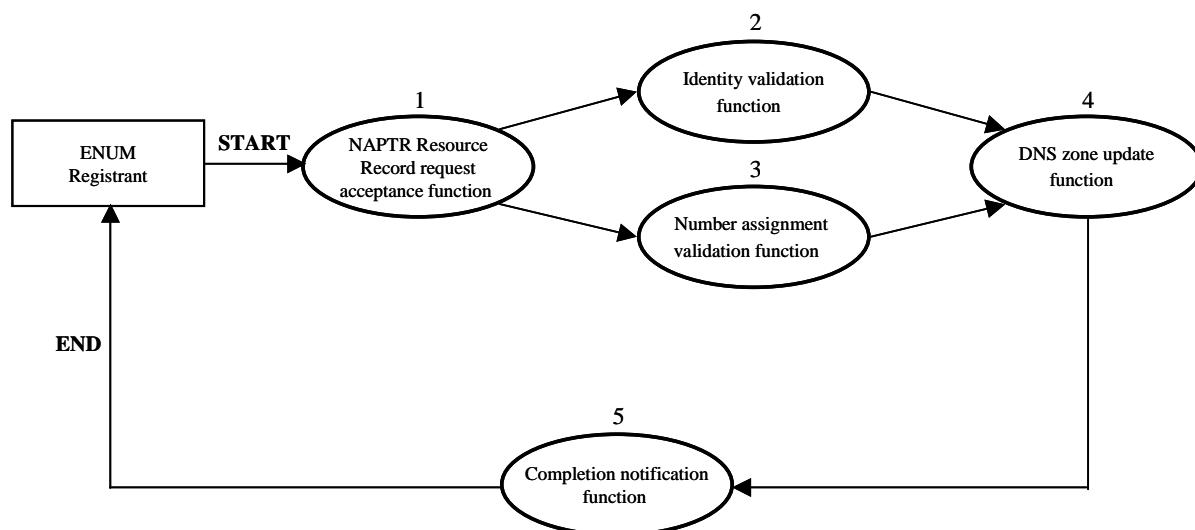
Figure 8 represents a functional model and should not be considered as a business model as variants may exist.

The following process takes place for the removal of E.164 numbers and NAPTR Resource Records from ENUM databases:

1) The **ENUM information removal request acceptance** step involves accepting requests from an ENUM Registrant (either an end user or an agent acting on behalf of an end user) or an Assignment Entity to remove information relating to an E.164 number from ENUM databases.

2) The **identity validation** step involves confirming:

   - the identity of an ENUM Registrant who is the ENUM end user; or

   - the identity of an ENUM Registrant who is not the ENUM end user and its authority to make a request on behalf of the ENUM end user; or

- the identity of an Assignment Entity and its authority to make a request in relation to a particular E.164 number.

3) The **number status validation** step involves confirming that the E.164 number is assigned to the ENUM end user or, prior to its relinquishment or withdrawal, was assigned to the ENUM end user.

4) The **DNS zone delegation withdrawal** step involves withdrawing the delegation of DNS authority to the zone corresponding to an E.164 number by removing the pointers to the URI corresponding to the number.

5) The **DNS zone deletion** step involves deleting ENUM information relating to an E.164 number from the DNS.

6) The **notification of completion** step involves informing the originator of the removal request that the removal process has been successfully completed.

11.3   Processes for changing Registrars

Requirements and procedures should exist to enable an ENUM Registrant to change the Registrar responsible for registration of the domain and creation of the NAPTR records corresponding to an E.164 number. These requirements and procedures should support change of Registrar in such a way that no interruption in an ENUM end user's use of the domain name and NAPTR records.

Where requirements and procedures for change of Registrar exist in a country in respect of normal Internet domain name registrations, these requirements and procedures should be checked to establish whether they meet the additional requirements that apply when an ENUM Registrar changes. Where no such requirements and procedures exist in a country the following points should be considered:

- an ENUM end user should be able to change Registrar at any time;

- an ENUM end user with domain name registrations and NAPTR records for more than one E.164 number should be able to change Registrar in respect of all or some of the numbers;

- a request to change Registrar should be made by an ENUM Registrant to its selected new Registrar;

- the new Registrar should validate the identity of the ENUM Registrant and, if the latter is not the ENUM end user, verifies its authority to act on behalf of the ENUM end user;

- the new Registrar should verify that the E.164 number is assigned to the ENUM end user;

- the new Registrar should notify the Tier 1 Registry and ENUM Tier 2 Nameserver Provider and the old Registrar of the intention of the ENUM Registrant to change Registrar;

- within a specified time, the Tier 1 Registry and ENUM Tier 2 Nameserver Provider should amend their Registrant information to identify the new Registrar as the Registrar of record for the particular ENUM Registrant, and notify the old and new Registrars of the amendments. It is the prime responsibility of the Tier 1 Registry to supervise the proper completion of the process;

- in the case that an unauthorized change of Registrar occurs, the ENUM Tier 2 Nameserver Provider should reverse the amendment of its Registrant information within a specified time. It may also be appropriate for penalties to be applied where an intentional unauthorized change of Registrar is attempted or occurs; and

- it may be appropriate to stipulate which entities, if any, may charge fees for change of Registrar, and how such fees may be established.

11.4   Other provisioning processes

In addition to the provisioning processes mentioned in clauses 11.2 and 11.3, the following provisioning processes:

- Changes or Modifications initiated by Registrant:

  - Renewal of ENUM Registration

  - Registrant changes ENUM Tier 2 Nameserver Provider

  - Registrant changes TSP

  - Registrant changes Contact Information

- Changes or Modifications initiated by Registrar:

  - Transfer to new Registrar

  - Transfer to new ENUM Tier 2 Nameserver Provider

  - Modification of Contact Information

- Changes or Modifications initiated by ENUM Tier 2 Nameserver Provider:

  - Transfer to new ENUM Tier 2 Nameserver Provider

  - Transfer to new Name Server

  - Modification of Contact Information

- Changes or Modifications initiated by Tier 1 Registry:

  - Transfer to new Tier 1 Registry

  - Transfer to new Name Server

- Changes or Modifications initiated by NNPA or TSP:

  - Opening up of new Numbering Range

  - Modification of existing Numbering Range

12   Considerations in development and assessment of options for national implementations

There are a number of generic points that are expected to be useful and relevant in the development and discussion of implementation options in all European countries, irrespective of the specific options considered and the country involved. The individual countries and the national parties they wish to involve are encouraged to consider the following points.

12.1   Validation

The validation of the relation between the E.164 number and the end user to which it is assigned as well as the status of an E.164 number is crucial in ENUM, see clauses 10 and 11. Validation is needed during the initial entering of a number in ENUM. Validation is also needed after a number has been entered, to ensure that the numbers in ENUM remain assigned. One of the goals in the development of an implementation for the administrative processes in ENUM may be to have a validation process that is simple while, at the same time, discourages fraud and unauthorized creation or transfer of services. Depending on the national telecommunications environment, the simplicity or complexity of the validation process may be an important criterion in the assessment of different implementation options.

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

- The Registrar relies for validation on an third party entity that holds information on the relation between an E.164 number and the end user to which it is assigned. Depending on the national telecommunications environment, this entity may be the Telephone Service Provider (TSP) that provides the telephony service for the number involved, or the NNPA in the case of numbers that are assigned directly to end users, or directory database operators. It is worth noting that, where this third party entity is a telephone service provider, it may be necessary for the Registrar to have a method available for determining which is the relevant telephone service provider to contact. Such a method may need to take special account of any ability of end users to port numbers from one service provider to another.

- The Registrar relies for validation on receiving an appropriate standard of documentary evidence from an ENUM registrant demonstrating that the end user has been assigned the E.164 number. Suitable documentary evidence might be a letter or digital certificate from the body that assigned the number to the end user that substantiates the assignment, or a bill from a telephony service provider that demonstrates that a telephone service is supplied in connection with the number. It may be necessary to take account of the age of possible types of documentation reducing their value.

These two options are illustrated below:
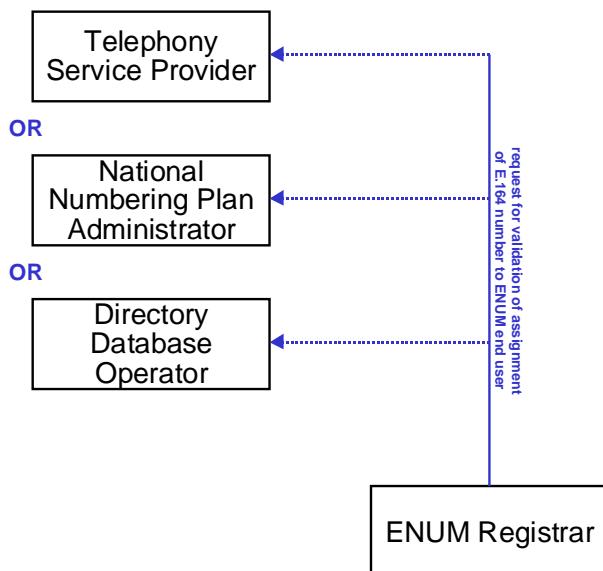
Figure 9: Validation of assignment via third party entity
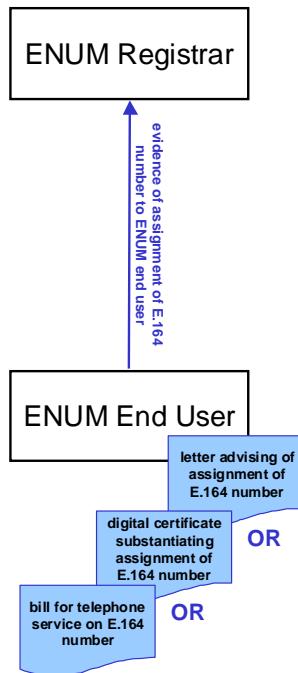
Figure 10: Validation of assignment via documentary evidence

In the case that an E.164 number is withdrawn, the number has to be removed from ENUM. In general, it is not always possible to rely on the ENUM registrant for the triggering of this removal process, see clause 11.2.3. Several ways may be available to ensure that numbers that are no longer assigned are removed from ENUM.

- One option may be for the entity that has the information on the relation between an E.164 number and the end user to trigger the removal process. This entity may be the telephone service provider that provides the telephony service for the number involved, the NNPA in the case of numbers that are assigned directly to end users, or directory database operators. This option is illustrated in figure 11.

- Another option may be to periodically check the assignment of the individual E.164 numbers in ENUM through repeating the processes used for the initial number validation process. When determining the frequency of revalidation the ageing period used between ceasing a number and reassigning it should be considered. In principle the revalidation period should be less than the ageing period.
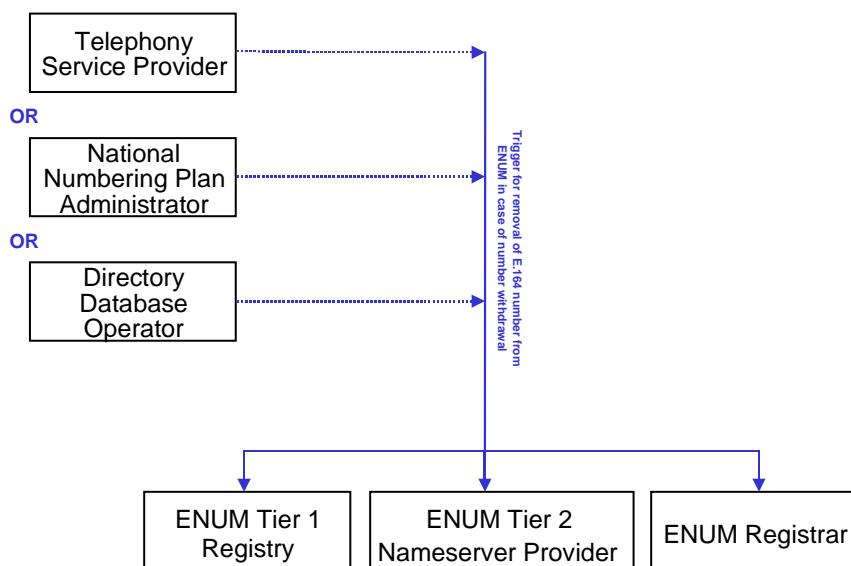
Figure 11: Triggering of the removal process by third party entity

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

12.2   Types of numbers

The numbering space behind a given E.164 country code is likely to encompass several categories of numbers, such as geographic, mobile, and service numbers. It is a national matter which of these categories are selected as candidates for inclusion in the national ENUM implementation.

12.3   Openness to competition

An implementation should allow for competition at every position where benefit can be achieved.

- The end user should be completely free in his choice of service providers for the subscriptions he can have in ENUM. In particular, the various subscriptions should not be coupled in order to prevent the occurrence of customer lock-in.

- There can be multiple competing ENUM Tier 2 nameserver providers /ENUM registrars (see table B.1).

- For technical reasons, the central registry for a country code in Tier 1 is likely to be a monopoly. The commercial environment in which this monopoly exists requires careful consideration. One way to control the power of the monopoly is to restrict its service offering. In this approach, the monopoly would be allowed to offer only the registry functions directly necessary for ENUM under precisely prescribed conditions. The exact functions and conditions are a national matter and expected to vary from national implementation to national implementation."

12.4   Complexity and effort associated with provisioning

It is expected to be useful to take into account the different types and amounts of interactions between the several entities in an implementation. For example, a distinction can be made between infrequent and frequent interactions. Infrequent interactions are carried out only once or, at most, only a few times, and involve many E.164 numbers at the same time. An example of an infrequent interaction is the DNS delegation from Tier 0 to Tier 1 for a country code-level ENUM domain. Frequent interactions, on the other hand, relate to individual E.164 numbers and are expected to occur many orders of magnitude more frequently. An example of a frequent interaction is the request by an end user to a registrar in Tier 2 to enter his number into ENUM.

13   Recommendation for ENUM implementation within Europe

- It is recommended that within Europe ENUM be implemented by use of the common designated .e164.arpa domain, or under another domain name branch that is recommended by the ITU.

- Full support is given for alignment with the final ITU-T/ISOC decision on this matter, and it is their view that implementation within a single second level domain, coupled with sound management and administration guidelines should be actively encouraged.

- The decision to participate in ENUM with the inclusion of E.164 national numbering resources in the DNS is a national matter.

- Within a common designated domain it is possible to sub delegate sections of the domain. See annex B. For Geographic Country Codes it is proposed that Europe follows the structure in the table in annex B.

- Insertion and deletion of users' numbers within ENUM should be the result of a positive decision to 'opt-in' by the user to whom the respective number is assigned.

- There is clearly no single option that is a best fit for all European countries. Each NRA should use the principles set out in the present document to develop an implementation that best meets their objectives.

- Administration implementation model at Tier 1 and Tier 2 is a national matter.

Annex A (informative):
Examples for grouping of functionalities in national implementations

A.0 Introduction

In this annex, the term "delegation" is used in a technical DNS or provisioning sense, and not in terms of delegation of responsibility (see clause 10 and annex B). Because of this, only the technical points of contact are shown in the examples and not the administrative points of contact.

The development of processes for the provisioning of records in Tier 1 and Tier 2 is a national matter. It is a task that member states are likely to perform together with the national parties they wish to involve. In essence, the task consists of:

1) Grouping the various functionalities needed in the national implementation. The core set of functionalities is given in clause 11. Depending on the national telecommunications environment, additional functionalities may be needed. It is expected to be useful to take the considerations listed in clause 12 into account in the determination of the grouping.

2) Assigning the responsibility for each group of functionalities to a suitable entity.

All implementations should provide the core functionalities listed in clause 11 so that the national ENUM implementations will integrate seamlessly and end users will experience one single European ENUM. Both the grouping of functionalities and the assignment of groups of functionalities to entities are expected to vary from European country to European country depending on different business models. However all implementations should adhere to the principles contained within the present document.

Each ENUM user will require a subscription to the ENUM function via an ENUM Registrar and where needed a DNS subscription.

Below are a number of example implementation options that may be useful to progress the thinking on European approaches to national ENUM implementations. The list of example options presented here is by no means exhaustive. The fact that an example option is presented here does not mean that it is considered to be more suitable, in any sense, than options not presented here.

The aspects of the implementation shown in figures A.1 to A.4 are:

- The assignment of the functions listed in clause 11.2.1 to the various entities in the implementation. These are the functions needed to enter an E.164 number into ENUM.

- The interactions between entities needed to enter an E.164 number into ENUM.

- The DNS delegation structure.

- The various subscriptions that the end user can have.

NOTE 1: The figures below only show the functions listed in clause 11.2.1 for the entering of E.164 numbers into ENUM. The allocation of the functions described in clauses 11.2.2 (amendment) and 11.2.3 (removal) to the different entities is very similar, therefore detailed descriptions are not provided. These processes are also initiated by the end user. There is one exception: the removal of an E.164 number from ENUM can also be initiated by the Assignment Entity if it withdraws the number, see clause 11.2.3.

NOTE 2: The figures show the process for the insertion of a single E.164 number, so multiple entities e.g. Tier 2 Nameserver Providers and Registrars are not shown.

A.1 Example 1

Figure A.1 shows an example implementation that uses a single Tier 1 Registry and a distinct ENUM Tier 2 Nameserver Provider and ENUM Registrar. It is assumed that there is a single Tier 1 Registry in a country, but it is left open as to which party or parties operate the Tier 1 Registry.

Figure A.1 only shows the functions listed in clause 11.2.1 and associated interactions for the entering of E.164 numbers into ENUM.

From top to bottom, the following entities are encountered:

- The ENUM Tier 0 Registry delegates the responsibility for the DNS zone c.c.e164.arpa to the Tier 1 Registry in the country with E.164 country code cc.

  - The Tier 1 Registry delegates the DNS zone responsibility for the E.164 number to the ENUM Tier 2 Nameserver Provider that stores the NAPTR records associated with that telephony number. The information needed for the delegation (name servers) is provided by the ENUM Tier 2 Nameserver Provider to the Tier 1 Registry through the ENUM Registrar.

  - The Assignment Entity is responsible for assignment of E.164 numbers in association with a telephony service. The assignment entity can be either the NRA or TSP depending on the rules for the assignment of E.164 resources. The Assignment Entity is involved in the validation of the E.164 number assignment.

  - The ENUM Tier 2 Nameserver Provider stores the actual NAPTR records for the end user.

  - The ENUM Registrar registers the ENUM domain name and its associated delegation information (i.e., ENUM Tier 2 Nameserver addresses) with the Tier 1 Registry on behalf of the end user. The ENUM Registrar will have to be accredited. The ENUM Registrar also undertakes the required validation functions (i.e. number assignment validation, user identity validation).

  - The end user has an ENUM subscription to the ENUM Registrar of his choice. The end user has also a commercial relationship with the ENUM Tier 2 Nameserver Provider (DNS Subscription) of his choice. In addition, the end user has a telephony subscription to the TSP of his choice that provides him with a telephony service. As an option, the end user can have a subscription to an Application Service Provider (ASP) of his choice that provides him with one or more ENUM-based services.

ENTITIES   FUNCTIONS

e164arpa
CC.e164arpa   ENUM Tier 0 Registry   See clause11 for functions

                    Prior delegation of DNS zone
                    corresponding to CC

                    Tier 1 Registry   5: DNS zone delegation function
CC.e164.arpa   CC.e164arpa

x.y... .CC.e164.arpa

Interaction D
Request for DNS   DNS zone delegation
zone delegation   for individual number
and confirmation   serviced by ENUM
                               Tier 2 Nameserver
                               Provicer   3: number validation function

Validation Entity   x.y... .CC.e164.arpa

Interaction C   NAPTR RR   1: NAPTR resource request function
request for   4: DNS zone creation function
number assign.   ENUM Tier 2
Validation and   Nameserver
confirmation   Provider

                                                               2: identity validation function
                                                               6: notification of completion function

ENUM Registrar   LEGEND
                                                               DNS zone delegation →
Interaction B   **Interaction A**
service   STOP: ENUM **Request insertion**   **Interactions between**
request + Tier 2 notif. of subscrip **of number &**   **entities to enter E.164**
nameserver   compl tion   **return ENUM Tier**   **number into ENUM**
provider info   **2 nameserver**
                               info
end user   **End user subscription**

                               DNS subscription

Figure A.1: Single Tier 1 Registry and separate ENUM Tier 2 Nameserver provider and
Registrar - Entering an E.164 number and NAPTR records in ENUM database

A.2   Example 2

Figure A.2 shows an example implementation that uses multiple Tier 1 Registries and a separate ENUM Tier 2 Nameserver Provider and ENUM Registrar. This means that the combined Tier 1 Registry function is formed by multiple entities, each of which is responsible for a specific part or the national numbering resource e.g. there is no overlap (or duplication) of numbers held within each Registry.

In this scenario, although there are multiple Tier 1 Registries within a country, it is left open as to which party or parties operate these Tier 1 Registries.

From top to bottom, the following entities are encountered:

- The ENUM Tier 0 Registry delegates the responsibility for the DNS zone x.c.c.e164.arpa to a Tier 1 Registry in the country with Rec. E.164 country code cc, where x represents a section or part of the national numbering scheme that has been delegated to a particular Tier 1 Registry. For example, in the UK 7.4.4.e164.arpa could be delegated to an entity performing a Tier 1 Registry function and this registry would be responsible for the ENUM implementation of all mobile numbers in the UK. This would require direct pointers from the Tier 0 Registry to each separate part of the Tier 1 Registry.

- The Tier 1 Registry delegates the DNS zone responsibility for a telephone number to the ENUM Tier 2 Nameserver Provider that stores the NAPTR records associated with that telephony number. The information needed for the delegation (name servers) is provided by the ENUM Tier 2 Nameserver Provider to the relevant Tier 1 Registry through the ENUM Registrar.

- An Assignment Entity is responsible for the assignment of E.164 numbers in association with a telephony service. The assignment entity can be either the NRA or TSP depending on the rules for the assignment of E.164 resources. The Assignment Entity is involved in the validation of the E.164 number assignment.

- The ENUM Tier 2 Nameserver Provider stores the actual NAPTR records for the end user.

- The ENUM Registrar registers the ENUM domain name and its associated delegation information (i.e., ENUM Tier 2 Nameserver addresses) with the relevant Tier 1 Registry on behalf of the end user. ENUM Registrars will have to be accredited by the relevant Tier 1 Registry.

- The ENUM Registrar has a trust relationship with the Registrant; that is, it must trust that the Registrant has authority over the ENUM domain name being registered. The ENUM Registrar may also work directly with the ENUM Tier 2 Nameserver provider to add or modify Nameserver information in the relevant Tier 1 Registry. To the extent that it does so it has a trust relationship; that is, it must trust that the ENUM Tier 2 Nameserver provider is acting on behalf of the Registrant.

- The end user has an ENUM subscription to the ENUM Registrar of his choice. Apart from this, the end user has a telephony subscription to the TSP of his choice that provides him with a telephony service. As an option, the end user can have a subscription to an Application Service Provider (ASP) of his choice that provides him with one or more ENUM-based services.
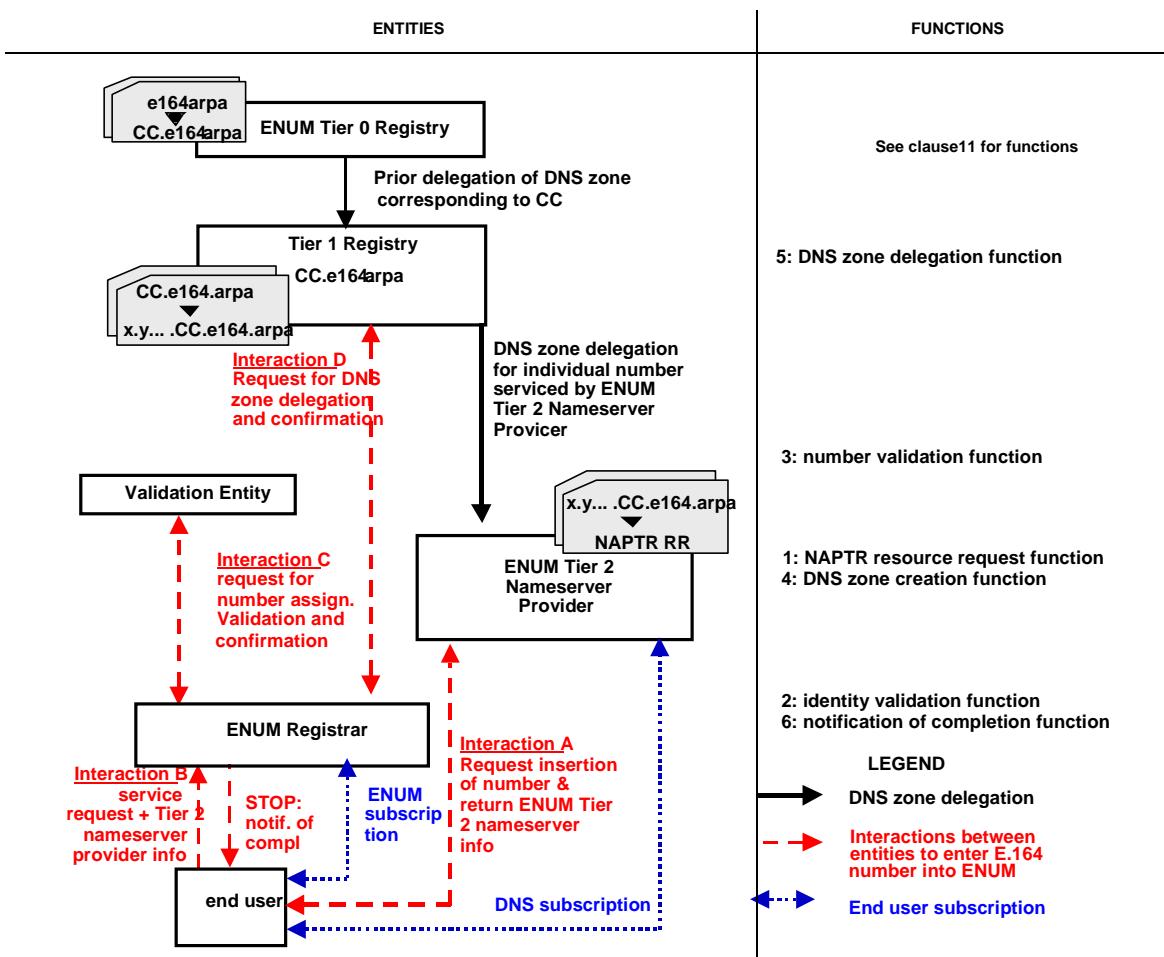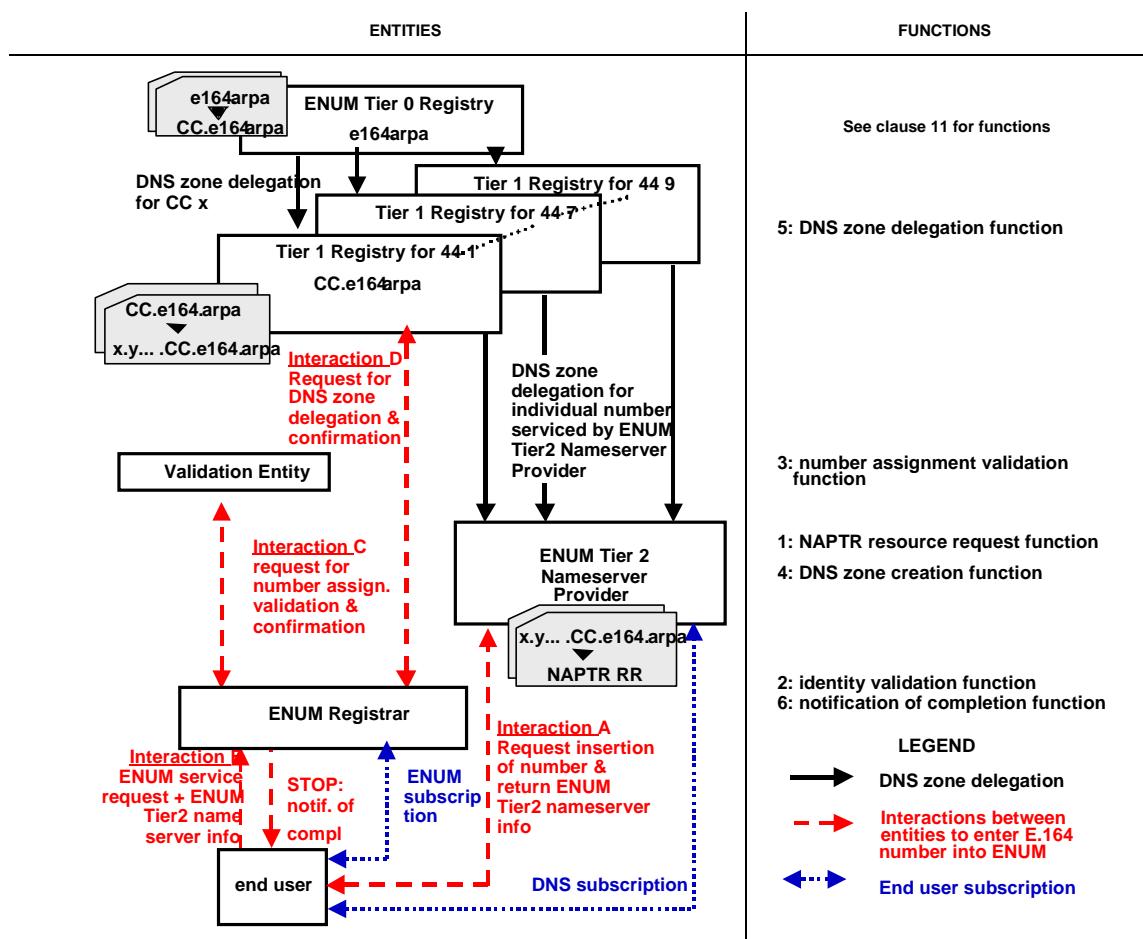
ENTITIES

FUNCTIONS

e164arpa

CC.e164arpa

ENUM Tier 0 Registry
e164arpa

See clause 11 for functions

**DNS zone delegation
for CC x**

Tier 1 Registry for 44 9

Tier 1 Registry for 44·7

**5: DNS zone delegation
function**

Tier 1 Registry for 44·1
CC.e164arpa

CC.e164.arpa

x.y... .CC.e164.arpa

**Interaction D
Request for
DNS zone
delegation &
confirmation**

**DNS zone
delegation for
individual number
serviced by ENUM
Tier2 Nameserver
Provider**

Validation Entity

**3: number assignment validation
function**

**Interaction C
request for
number assign.
validation &
confirmation**

**ENUM Tier 2
Nameserver
Provider**

1: NAPTR resource request function

4: DNS zone creation function

x.y... .CC.e164.arpa

NAPTR RR

2: identity validation function
6: notification of completion function

ENUM Registrar

LEGEND

**Interaction B
ENUM service
request + ENUM
Tier2 name
server info**

**STOP:
notif. of
compl**

**ENUM
subscrip
tion**

**Interaction A
Request insertion
of number &
return ENUM
Tier2 nameserver
info**

DNS zone delegation

**Interactions between
entities to enter E.164
number into ENUM**

end user

DNS subscription

End user subscription

**Figure A.2: Multiple Tier 1 Registries and separate ENUM Tier 2 Nameserver Provider and
Registrar - Entering an E.164 number and NAPTR records in ENUM database**

A.3   Example 3

Figures A.3 illustrates an example national implementation of ENUM administration that features a single Registry that combines Tier 1 and Tier 2, and a separate ENUM Registrar that operates at both Tier 1 and Tier 2.

This means that, within a given country, there is a single entity providing registry services and one or more entities providing registrar services.

The following entities appear in figure A.3.

- a prior delegation of responsibility for the DNS zone corresponding to an E.164 country code is made by the Tier 0 Registry. In the case of integrated numbering plans the delegation is either of the complete DNS zone corresponding to the country code, or of the DNS zone corresponding to a national portion of the country code;

- the Tier 1 Registry + ENUM Tier 2 Nameserver Provider receives the delegation of responsibility for the DNS zone corresponding to an E.164 country code or a national portion of a country code from the ENUM Tier 0 Registry. The Tier 1 Registry + ENUM Tier 2 Nameserver Provider also creates and deletes domains corresponding to an E.164 number, and creates, amends and deletes NAPTR records associated with that number.
  For reasons of quality of service and consumer safeguards, it is envisaged that the Responsible Administrative Organization for the Domain would accredit the Tier 1 Registry +ENUM Tier 2 Nameserver Provider.
  The ENUM Subscriber holding the number will have a DNS subscription with the Tier 1 Registry + ENUM Tier 2 Nameserver Provider;

- the ENUM Registrar validates the identity of the ENUM Registrant and, if the latter is not the ENUM Subscriber, verifies its authority to act on behalf of the ENUM Subscriber. The ENUM Registrar also validates the assignment of the number to the ENUM Subscriber, registers and de-registers the domain name corresponding to an E.164 number with the Tier 1 Registry + Tier 2 Nameserver Provider, and specifies the information for creation, amendment and deletion of NAPTR records.
  For reasons of quality of service and consumer safeguards, it is envisaged that the Designated Manager would accredit ENUM Registrars. It is also envisaged that, for competition reasons, the Tier 1 Registry + ENUM Tier 2 Nameserver Provider would not be permitted to operate as a Registrar.
  If an ENUM Registrar acting in relation to a particular number is an Application Service Provider, the end user holding the number will have an ENUM-dependent service subscription with that Application Service Provider;

- the Assignment Entity validates the assignment of an E.164 number. In the case that the assignment of a number ceases, the Assignment Entity may also request an ENUM Registrar to remove ENUM information corresponding to that number.
  If the Assignment Entity for a particular number is a Telephony Service Provider, the end user holding the number will have a telephony service subscription with that Telephony Service Provider; and

- the ENUM Registrant requests an ENUM Registrar to create or remove domains corresponding to an E.164 number, and to create, amend or delete NAPTR records.
  If an ENUM Registrant is an Application Service Provider, the end user holding the number will have an ENUM-dependent service subscription with that Application Service Provider. If an ENUM Registrant is the end user, it will have a DNS subscription with the ENUM Tier 1 Registry + ENUM Tier 2 Nameserver Provider, a telephony service subscription with a Telephony Service Provider, and may have an ENUM-dependent service subscription with an Application Service Provider.

Features of this implementation are:

- the reduction in the number of Registry entities, due to the combination of Tier 1 Registry and ENUM Tier 2 Nameserver Provider;

- the consequential elimination of delegations from Tier 1 to Tier 2;

- requests for domain and NAPTR resource creation, and for NAPTR resource amendment, are initiated by the ENUM Registrant;

- requests for domain and NAPTR resource deletion are initiated by the ENUM Registrant or the Assignment Entity;

- the identity of the ENUM Registrant is validated by the ENUM Registrar (including, if applicable, its authority to act on behalf of the ENUM Subscriber holding an E.164 number) before responding to any request for domain and NAPTR resource creation, amendment or deletion;

- the assignment of the E.164 number to the end user is validated by the ENUM Registrar with the Assignment Entity before responding to any request for domain and NAPTR resource creation; and

- information necessary for creation and deletion of domains and NAPTR records corresponding to an E.164 number, and for amendment of NAPTR records corresponding to a number, is prepared by the ENUM Registrar and provided to the Tier 1 Registry + ENUM Tier 2 Nameserver Provider.
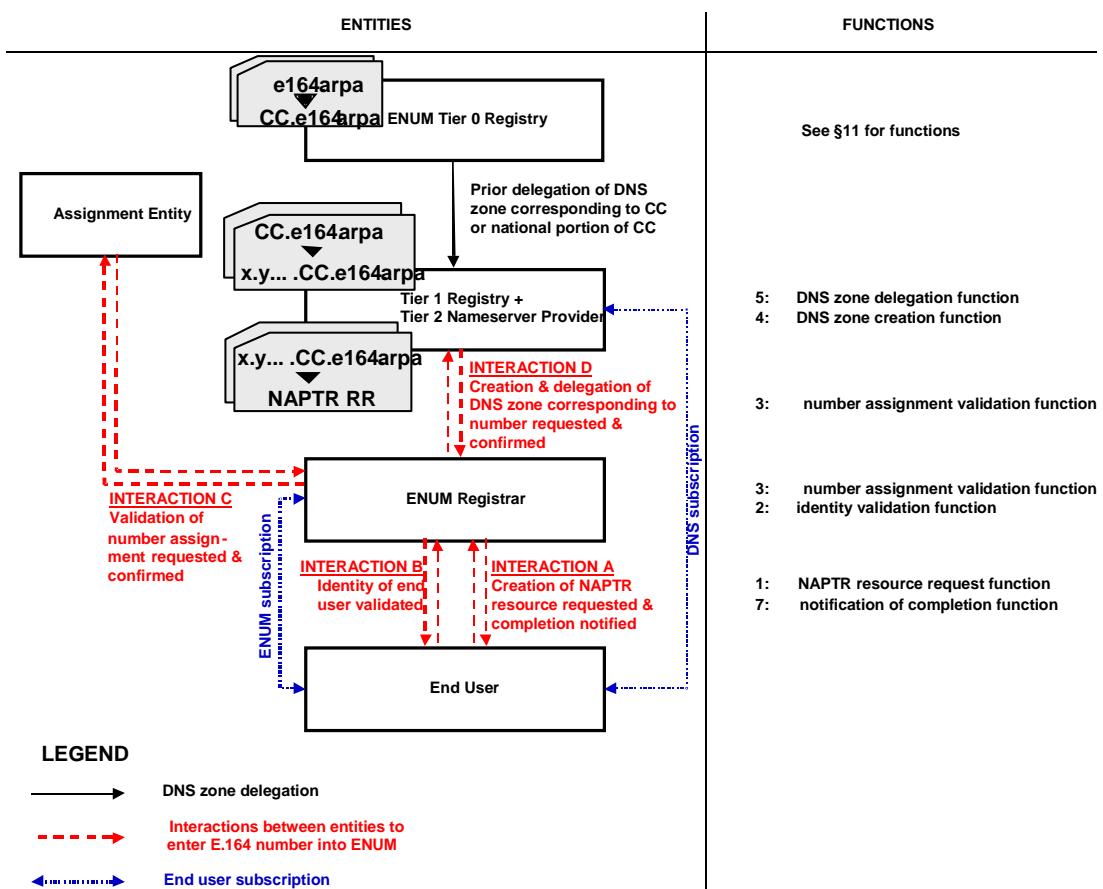
Figure A.3: Combined ENUM Tier 1 and 2 and separate ENUM Registrar - Entering an E.164 number and NAPTR records in ENUM database

A.4   Example 4

Figure A.4 shows an example implementation that uses a two-stage Tier 1 approach. This means that the Tier 1 is formed by two separate entities, the Tier 1 Registry part A (T1R-A) and Tier 1 Registry part B (T1R-B). It is assumed that there is a single T1R-A in a country, but it is left open as to which party or parties operate the T1R-A. The T1R-B role is performed by the parties that manage individual telephony subscriptions and have the information needed for the number assignment validation. Among the candidates for the T1R-B role are telephony service providers that have been assigned numbers for distribution among end users. It is expected that in most European countries, there are many T1R-Bs. Furthermore, any party can become an ENUM Tier 2 Nameserver Provider and Registrar (T2NPR), so it is expected that that there are also many T2NPRs.

From top to bottom, the following entities are encountered:

- The ENUM Tier 0 Registry delegates the responsibility for the DNS zone c.c.e164.arpa to the T1R-A in the country with Rec. E.164 country code cc. In case of integrated numbering plans, the delegation is either of the complete DNS zone corresponding to the country code, or of the DNS zone corresponding to a national portion of the country code.

- The T1R-A delegates the DNS zone responsibility for each telephone number to the T1R-B that manages the telephony subscription for that individual telephone number. The delegation is not based on number blocks, as individual numbers in a block can be ported because of number portability for E.164 numbers. Instead, the delegation is done for groups of individual numbers for which the telephony subscriptions are managed by a given T1R-B. Together, the T1R-A and T1R-Bs perform the ENUM Tier 1 Registry function from table 1 in annex B.

- The T1R-Bs, in turn, delegate the DNS zone responsibility for a telephone number to the T2NPR that provides the ENUM service for that telephony number. The information needed for the delegation is provided by the T2NPR.

- The T2NPR stores the actual NAPTR records for the end user and provides the ENUM registration functions to the end user. Each T2NPR thus performs the ENUM Tier 2 Nameserver Provider and ENUM Registrar functions from table 1 in annex B. Note that it is very well possible to split the T2NPR and create separate entities for the nameserver provider and registrar functions.

- The end user has an ENUM subscription to the T2NPR of his choice. Apart from this, the end user has a telephony subscription managed by the T1R-B of his choice. As an option, the end user can have a subscription to an Application Service Provider (ASP) of his choice that provides him with one or more ENUM-based services.

The T1R-A does not need to know which telephone numbers are managed by which T1R-B. Instead, this information is provided by the T1R-B for the telephone numbers for which this T1R-B manages the telephony subscription. The T1R-B thus defines the groups of numbers for which the delegation is performed. The delegation for the groups of numbers from T1R-A to T1R-B (function 5a) can be performed before the request for the delegation for an individual number from T1R-B to T2NPR is received (function 5b).

The validation of the relation between a telephone number and a telephony subscriber is T1R-B-internal. For each number that a T1R-B manages the telephony subscription for, the T1R-B either knows the end user by name or has other ways to determine the assigned use of the number.

After a number has been entered into ENUM, it is likely that at some stage, the number needs to be removed or the associated NAPTR records need to be amended. The triggers for the amendment and removal processes can originate from two entities:

- The T1R-B. The removal of an E.164 number from ENUM is required if the assignment entity withdraws the number, for example if the telephony service to that number is terminated, see clause 11.2.3.

    - If a number is assigned to the end user by the T1R-B, the detection of the withdrawal and the termination of the telephone service is T1R-B-internal and the T1R-B initiates the removal process.

    - If a number is assigned to the end user by a separate assignment entity, the T1R-B managing the telephony subscription for that number is notified of the withdrawal. This notification is part of the existing procedures in telephony number management, independent from ENUM. After receiving the notification, the T1R-B initiates the removal process.

- The end user. The end user can at any time choose to amend his NAPTR records or remove his number from ENUM.

The rationale behind the two-stage Tier 1 approach is keep the number of interactions and the overall work effort in the implementation limited by exchanging information directly and locally.
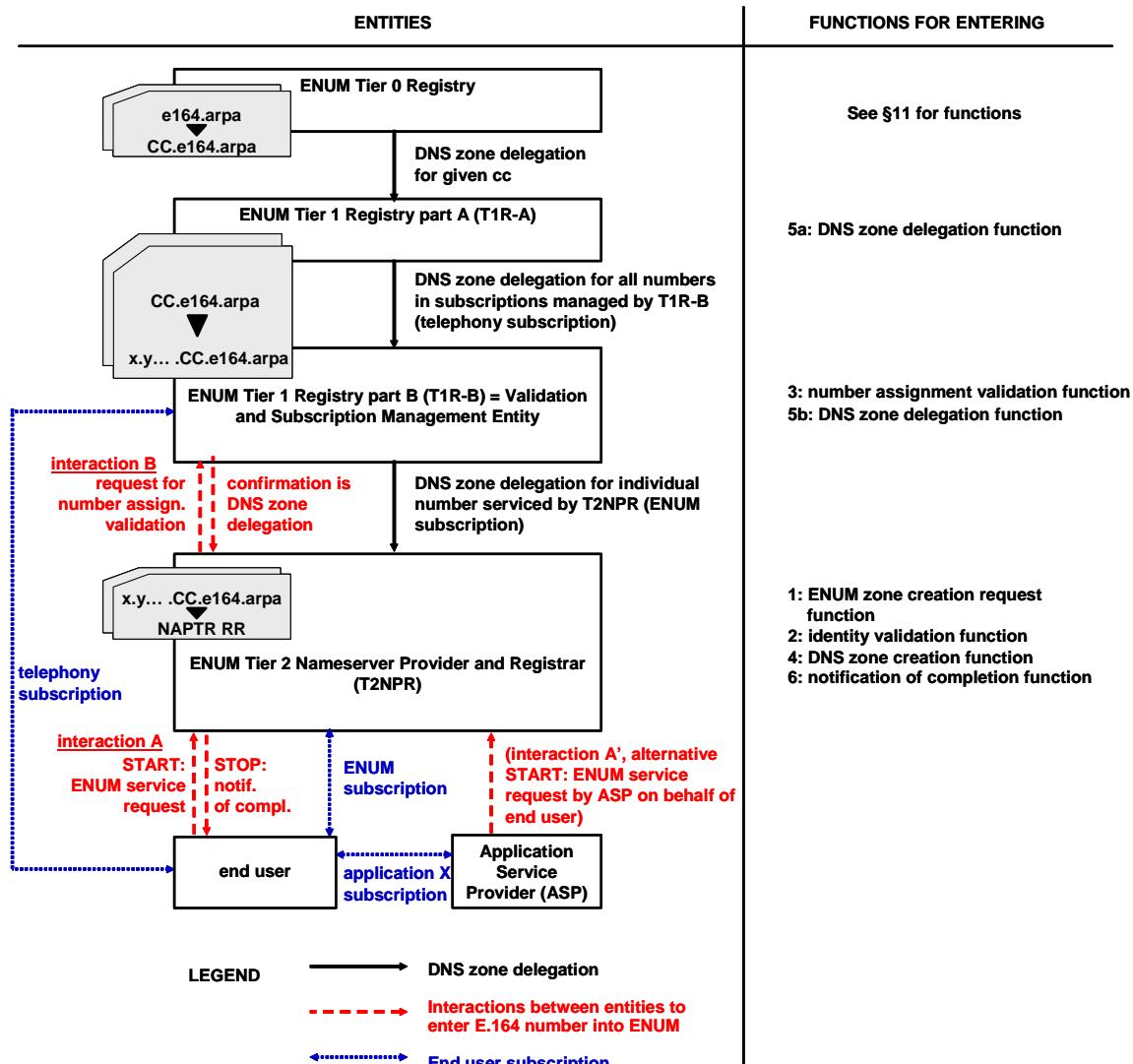
Figure A.4: Two-stage Tier 1 with combined ENUM Tier 2 Nameserver Provider and Registrar - Entering an E.164 number and NAPTR records in ENUM database

Annex B (informative):
ENUM entities - functions and responsibilities

Table B.1: ENUM entities functions and responsibilities

Domain	Responsible administrative organization for the domain (*Designated manager*)	Responsible technical organization for the domain (*Registry*)	Registrar	Delegations from zone made to
"." (DNS Root level)	**DNS Root Manager** ICANN through agreement (see note 1) with U.S. DoC	**DNS Root Registry** IANA, which is part of ICANN	**DNS Root Registrar** N/A	N/A
.arpa (TLD level)	**TLD Manager** Entity responsible for managing the TLD level.	**TLD Registry** Entity designated by the TLD Manager.	**TLD Registrar**	
.e164.arpa (ENUM Root level)	**ENUM Tier 0 Manager** Entity responsible for managing the ENUM Root level.	**ENUM Tier 0 Registry** Entity designated by the ENUM Tier 0 Manager.	**ENUM Tier 0 Registrar** ITU TSB	The Registrant will be the ITU Member states or the NRA.
<CC>.e164.arpa (ENUM CC level)	**ENUM Tier 1 Manager** The ITU Member state (see note 2) who has been assigned the CC. The member state can delegate this responsibility to the NRA or other appropriate entity.	**ENUM Tier 1 Registry** The ITU Member state or the NRA can manage this in their own activities or designate someone else act as the ENUM Tier 1 registry.	**ENUM Registrar**	
.<N(S)N>.<CC>.e164.arpa (ENUM E.164 number level)	**ENUM Tier 2 Manager** ENUM end user - i.e. *national matter*	**ENUM Tier 2 Nameserver Provider**	**ENUM Registrars** - could be a TSP or other ENUM service provider - i.e. *national matter*.	The registrant will be the ENUM end user
NOTE 1: According to section III B (i-v) in MoU between U.S. DoC and ICANN (http://www.icann.org/general/icann-mou-25nov98.htm) and according to section 1 in agreement between USC and ICANN (http://www.icann.org/general/usc-icann-transition-agreement.htm).				
NOTE 2: For integrated numbering plans other procedures might apply.				

Annex C (informative):
DNS Concepts

The following text is offered as additional background information to help understanding of DNS terms and definitions, because of the close relationship between ENUM and the DNS.

C.1   DNS related definitions

Domain Name System: The *Domain Name* System (DNS) is a distributed Internet service arranged hierarchically. DNS is used mostly to translate between *domain names* and IP addresses, to control Internet email delivery and other purposes. It comprises of three components: the *name space*, the *name servers* making that name space available and *resolvers* (clients), which query the servers about the name space.

Name space: Domain Name Space: All combinations of *Domain Names* and *Top Level Domains* existing below the *Root*.

Zone: Any *domain name* that has been delegated by an *ancestor* zone. A zone is a point of delegation in the DNS tree. It contains (includes) all descendant *domain names* from a certain point downward that have not been *delegated* (because for those *delegated* other zones are *authoritative)*. A zone is therefore a discreetly managed portion of the total *Domain Name Space* within a single *domain* and is represented by the data stored on a particular *name server*. A zone is the part of a DNS domain for which the *register* contains information and for which the *name server* is *authoritative*.

Subdomain: Any child of a *domain zone*.

Label: An element of a **domain name**. No label can be longer then 63 characters. Labels are made up of letters, numbers and hyphens, but may not start with hyphens. Labels in a *domain name* are separated from each other by "."'s. Labels are case insensitive.

Fully Qualified Domain Name: A *domain name* that extends all the way back to *root*. Often written as FQDN. A common error is to leave the "." at the end off.

Delegation: The process of separating a descendant of a *zone* into a separate *zone*. The delegation is accomplished with *NS Records* (a type of a *resource record*).

Resource Record: One unit of data in the DNS. A resource record defines some attribute for a domain name such as an IP address, a string of text, or a mail route.

NS Record: Name Server Record. An NS record declares that a given *zone* is served by a given *name server*. Every NS record is either a *delegation* record or an *authority* record. If the name of the NS record is the name of the *zone* it appears in, it is an *authority* record. If the name of the NS record is that of a descendant zone, then it is a *delegation* record.

SOA Record: Start of Authority Record. The SOA is the first record in every properly configured *zone*. The SOA record contains information about the *zone* in a string of fields. The SOA record tells the server to be *authoritative* for the *zone*.

NAPTR Record: A DNS Resource Record that specifies a regular expression based rewrite rule that, when applied to an existing string, will produce a new domain label or Uniform Resource Identifier (URI).

Authoritative: Adjective describing a *name server*. The authoritative server contains an entire copy of the *zone* that is derived from local configuration data, possibly with the help of another authoritative name server for the zone. A server can be authoritative about one zone, but not authoritative for another.

Name Server: A name server is software that runs on a *host* that can be set to *authoritatively* answer queries for records in a *zone*.

Host: A host is any machine on any network. On TCP/IP networks, each host has one or more unique IP addresses.

Root Server: There are currently 13 servers that are *authoritative* for the *root zone*. They are named a.root-servers.net - m.root-servers.net. Every *resolver* must have the IP addresses of one or more of these root servers coded in so that it can resolve *domain names*.

Root Zone: The ancestor of all zones, the parent of the *top level domains*. It is written as ". ". *Root* (as it is often called) has no *labels*.

Resolver: A resolver is a host capable of performing a recursive search of the DNS to locate records that would answer a query. It does this by querying *name servers*, including the *root servers*. In other words, a resolver is a DNS server that looks up DNS records on behalf of a client machine.

Top Level Domain: Any *zone* owned by the *root servers*. You can also think of this as the first *label* in any domain name other than *root* (which has no *labels*).

Primary Server: Also called a master server. An *authoritative name server* that gets its *zone* data from local configuration, not from an outside source. This term is used in terms of a specific *zone*. The primary server of one *zone* could be a *secondary server* in regards to another *zone*. Despite a common misconception, from a *resolvers* point of view, primary and secondary servers are equal in authority and priority.

C.2   DNS administration related definitions

Registrant: The individual or organization that registers a specific *domain name* with a *registrar*. This individual or organization holds the right to use that specific *domain name* for a specified period of time, provided certain conditions are met and the registration fees are paid. This person or organization is the "legal entity" bound by the terms of the Domain Name Registration Agreement with the registrar. After successful registration this entity is the *Domain Name Holder*.

Domain Name Holder: see *Registrant.*

Registrar: A registrar provides direct services to *domain name registrants*. The registrar database contains customer information in addition to the DNS information contained in the *Registry* database. Registrars process name registrations for Internet end-users and then send the necessary DNS information to a *Registry* for entry into the centralized *Registry* database (*register*) and ultimate propagation over the Internet.

Registry: A domain name registry is an entity that receives domain name service (DNS) information from domain name *registrars*, inserts that information into a centralized database (*register*) and propagates the information in a *zone file* to the *primary name server* of this *zone*.

Register: The *registry* database. It contains only domain name service (DNS) information (*domain name*, *name server names* and *name server* IP addresses) along with the name of the *registrar* that registered the name and basic transaction data. It does not contain any domain name *registrant* or *contact information*. *Registrars* provide direct services to *registrants*.

Zone File: A file that contains data describing a portion of the domain name space. Zone files contain the information needed to resolve *domain names* to Internet Protocol (IP) numbers.

Contact Information: Contacts are individuals or entities associated with *domain name records*. Typically, third parties with specific inquiries or concerns will use contact records to determine who should act upon specific issues related to a domain name record. There are typically three of these contact types associated with a domain name record, the *Administrative contact*, the *Billing contact* and the *Technical contact*.

Contact, Administrative: The administrative contact is an individual, role or organization authorized by *the domain name holde*r to interact with the *registry* or *registrar* on behalf of the Domain Name Holder. The administrative contact should be able to answer non-technical questions about the domain name's registration and the *Domain Holder*. In all cases, the Administrative Contact is viewed as the **authoritative point of contact** for the domain name, second only to the Registrant.

Contact, Billing: The billing contact is the individual, role or organization designated to receive the invoice for domain name registration and re-registration fees.

Contact, Technical: The technical contact is the individual, role or organization that is responsible for the technical operations of the *delegated zone*. This contact likely maintains the *domain name server(s)* for the *domain*. The technical contact should be able to answer technical questions about the *domain name*, the *delegated zone* and work with technically oriented people in other zones to solve technical problems that affect the domain name and/or zone.

WHOIS: a TCP transaction based query/response server, that providing netwide directory service to network users. The WHOIS Protocol was originally defined in IETF RFC 954 [6]. The initial domain name related application layer implementations were centralized systems run by SRC-NIC and then later InterNIC/Network Solutions. The SRI-NIC and InterNIC implementations are more formally referred to as "NICNAME/WHOIS" services. WHOIS is not purely a domain name or IP address directory service, but has been deployed for a wide variety of uses, both public and private. Other variants of this service include RWHOIS and the newer Verisign Referral LDAP WHOIS service. WHOIS can refer to the protocol defined in IETF RFC 954 [6] or the generic application service described above.

Annex D (informative):
Bibliography

- ETSI TS 102 055: "Services and Protocols for Advanced Networks (SPAN); Scenarios for User and Infrastructure ENUM".

- ITU-T Recommendation E.190: "Principles and responsibilities for the management, assignment and reclamation of E-series international numbering resources".

- Further on work is going on an ITU-T Recommendation, E.A-ENUM "Principles and procedures for the administration of E.164 geographic country codes for registration into the domain name system".

- IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".

- IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

History

Document history		
V1.1.1	July 2002	Publication