

# **US Provider ENUM Tier 0/1 Registry Technical and Operational Requirements**

February 21, 2007

CC1 ENUM LLC

## **CC1 ENUM Provider Tier 0/1 Registry Technical and Operational Requirements for a Specific Country within Country Code 1**

CC1 ENUM LLC

### **Abstract**

This document contains technical and operational requirements for operating a Provider ENUM Tier 0/1 for the United States. This includes interfaces to other entities providing services for ENUM as well as the requirements for deploying and operating the ENUM Tier 0/1 infrastructure.

▪ **FOREWORD**

---

## ▪ SECTION 1.0 SCOPE, PURPOSE, AND APPLICATION

---

### *1.1 Scope*

This document describes the Provider ENUM Tier 0/1 technical and operational requirements for a specific country within the North American Numbering Plan (NANP) Country Code 1 serving area. In particular these technical requirements are to be used to select the Provider ENUM Tier 0/1 Registry operator for US telephone numbers (TNs) under the ITU-T E.164 international numbering standard, and may be accepted or modified by other NANP member nations when determining their approach.

Provider ENUM is defined as the use of the technology in RFC3761 by the Service Provider of Record (SPR) for a specific E.164 number to map a telephone number into a URI (Universal Resource Identifier) that identifies a specific point of interconnection to that service provider's network that could enable the originating party to establish communication with the associated terminating party. It is separate from any URIs that the end-user, who registers their E.164 number, may wish to associate with that E.164 number. Provider ENUM is sometimes referred to as "Carrier ENUM" or "Infrastructure ENUM".

The Provider ENUM Tier 0/1 Registry operator is the single entity responsible for providing Provider ENUM Registry services initially under e164enum.us and eventually under a global ENUM root (to be determined by the ITU-T<sup>1</sup>) for US TNs, including management of pointers to Tier 2 Provider name servers. The Tier 0/1 Registry does not contain Naming Authority Pointer (NAPTR) records but points at Tier 2 Providers where NAPTR records associated with E.164 numbers are stored. The ENUM Tier 0/1 Registry operator must establish an open standard interface that is available for all SPRs to use.

These requirements do not presume integration of User and Provider ENUM, for example, by sharing of common infrastructure components but also are not intended to preclude such sharing.

### *1.2 Purpose*

This document is intended to provide the specifications necessary to implement the Provider ENUM Tier 0/1 Registry for Numbering Plan Area (NPA) resources within the U.S. It is intended to provide sufficient information to allow the LLC to issue an RFP for an ENUM Tier 0/1 Registry implementation. As such, it describes, among other things, the reference architecture for the Provider ENUM Tier 0/1 Registry. It also provides the critical security and privacy requirements for implementing this system for the US numbering space.

This document will be distributed to all stakeholders with a view of seeking consensus amongst an audience that is as large as possible and ensuring that the implementation of a US ENUM Tier 0/1 Registry proceed as swiftly and as smoothly as possible.

### *1.3 Application*

This document is intended to be used as the basis for an RFP that will identify and provide the technical specifications necessary to select a vendor that will implement the Provider ENUM Tier 0/1 Registry for NPA resources within the U.S. This may also be used by other countries within the NANP for their ENUM Tier 0/1 Registry vendor selection requirement.

---

<sup>1</sup> Originally the IETF planned to use ie164.arpa for this purpose. That domain is used in this document as a placeholder until such time as a global apex for Provider ENUM is chosen.

## ▪ SECTION 2.0 REFERENCES

---

The following references contain provisions that, through reference in this text, constitute provisions of these technical requirements. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the references indicated below.

- [1] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.
- [2] Harrenstien, K., Stahl, M. and E. Feinler, "NICNAME/WHOIS", RFC 954, October 1985.
- [3] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
- [4] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
- [5] Mockapetris, P., "DNS encoding of network names and other types", RFC 1101, April 1989.
- [6] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.
- [7] Ohta, M., "Incremental Zone Transfer in DNS (IXFR)." RFC 1995, August 1996
- [8] Vixie, A P., "Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)." RFC 1996, August 1996
- [9] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
- [10] Vixie, A P., Ed., S. Thomson, Y. Rekhter, and J. Bound "Dynamic Updates in the Domain Name System (DNS UPDATE)" RFC 2136, April 1997
- [11] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.
- [12] Elz, R., Bush, R., Bradner, S. and M. Patton, "Selection and Operation of Secondary DNS Servers", BCP 16, RFC 2182, July 1997.
- [13] M. Horowitz & S. Lunt, "FTP Security Extensions" RFC 2228, October 1997.
- [14] Eidnes, H., de Groot, G. and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.
- [15] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.
- [16] M. Allman & S. Ostermann, "FTP Security Considerations," RFC 2577, May 1999.
- [17] Vixie, P., "Extension Mechanisms for DNS (EDNS0)." RFC 2671, August 1999
- [18] R. Bush, D. Karrenberg, M. Kosters, & R. Plzak, "Root Name Server Operational Requirements," RFC2870, June 2000.
- [19] Crawford, M. and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering." RFC 2874, July 2000
- [20] Eastlake, D., "DNS Request and Transaction Signatures (TSIG(0)s)." RFC 2931, September 2000
- [21] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures", RFC 3405, October, 2002
- [22] Crispin, M., "Internet Message Access Protocol, Version 4rev1", RFC 3501, March 2003.
- [23] ENUM Forum Final Specifications Document "ENUM Forum Specifications for US Implementation of ENUM Document" 6000\_1\_0, March 14, 2003
- [24] Hollenbeck, S., "Extensible Provisioning Protocol", RFC 3730, March 2004 .
- [25] Hollenbeck, S., "Extensible Provisioning Protocol Domain Name Mapping", RFC 3731, March 2004.
- [26] Hollenbeck, S., "Extensible Provisioning Protocol Host Mapping", RFC 3732, March 2004.
- [27] Hollenbeck, S., "Extensible Provisioning Protocol Contact Mapping", RFC 3733, March 2004.
- [28] Hollenbeck, S., "Extensible Provisioning Protocol Transport Over TCP", RFC 3734, March 2004.
- [29] Falstrom, P., Mealling, M., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.
- [30] RFC 2845
- [31] ICANN, "Uniform Domain Name Dispute Resolution Policy", Policy Adopted: August 26, 1999
- [32] ICANN, "Rules for Uniform Domain Name Dispute Resolution Policy", Policy Adopted: August 26, 1999
- [33] Hollenbeck, S. "E.164 Number Mapping for the Extensible Provisioning Protocol (EPP)," RFC 4114, June, 2005.

▪ **SECTION 3.0**      **DEFINITIONS, ACRONYMS, & ABBREVIATIONS**

---

**3.1**    *Definitions*

Address of Record	A URI that can be used to determine a point of interconnection with Service Provider of Record of the telephone number
Authentication	The process of verifying that a party, e.g., the Service Provider of Record, is who they claim to be. (See Verification)
Authorization	The process of verifying that an (authenticated) party is entitled to perform some action.
Core Registry Services	The three core services provided by the Registry - SRS, Name server, and ContactInfo Services
Core Internet Service Failure	Is an extraordinary and identifiable event beyond the control of Registry Operator affecting the Internet services to be measured pursuant to SLRs. Such events include but are not limited to congestion, collapse, partitioning, power grid failures, and routing failures
Cross Network Name Server Performance (CNNP) Test	Measurements conducted by sending strings of DNS request packets from each of four measuring locations to each of the Tier 0/1 name servers and observing the responses from the Tier 0/1 name servers. (These strings of requests and responses are referred to as a "CNNP Test".)
Dynamic Delegation Discovery System (DDDS)	Used to implement lazy binding of strings to data, in order to support dynamically configured delegation systems such as ENUM is based on. The DDDS functions by mapping some unique string to data stored within a DDDS Database by iteratively applying string transformation rules until a terminal condition is reached. (RFC 3401 to 3405)
ENUM	Refers to a protocol developed in the Internet Engineering Task Force (IETF) (RFC 3761) whereby the DNS can be used for identifying available services associated with one E.164 number
ENUM Tier 1A Registry	Organization that registers ENUM domains corresponding to NPAs and hosts the set of their authoritative name server (NS) records.
Provider ENUM	Use of the technology in RFC3761 by the carrier-of-record for a specific E.164 number to map a telephone number into a URI that identifies a specific point of interconnection to that service provider's network that could enable the originating party to establish communication with the associated terminating party

Provider ENUM Tier 0/1 Registry	The repository of ENUM domain name registrations for Provider ENUM
Provider ENUM Tier 0/1 Registry Operator	Organization that registers ENUM domains corresponding to 10 digit E.164 numbers for their Service Providers of Record and hosts the set of pointers to their Tier 2 name servers
Registry Data	Registration Data maintained by the Registry including Zone-File Data, and all other data submitted by SPRs
Service Provider of Record (SPR)	The service provider, recognized by the appropriate regulatory authority, which has been allocated numbering resources, as reflected in the LERG™ and NPAC.
Thick Registry	Is one in which all of the information associated with registered entities, including both technical information (information needed to produce zone files) and social information (information needed to implement operational, business, or legal practices), is stored within a central registry repository
Tier 2 Provider	Person/organization that maintains ENUM zone including the NAPTR resource records for that number and is pointed to by the Tier 0/1

### 3.2 *Acronyms & Abbreviations*

AAA	Authentication, Authorization and Accounting
ASCII	American Standard Code for Information Interchange
ASP	Application Service Provider
CC1	Country Code 1
CC1 ENUM LLC	Country Code 1 ENUM Limited Liability Corporation
CNAME	Canonical Name
CNNP	Cross Network Name Server Performance
CRISP	IETF Cross Registry Information Service Protocol Working Group
CSR	Customer Service Representatives'
DDDS	Dynamic Delegation Discovery System
DNS	Domain Name System
DNSSEC	DNS Security Extension
ENUM	TElephone NUmber MAPPING
EPP	Extensible Provisioning Protocol
FCC	Federal Communications Commission
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HVAC	Heating, Ventilating, and Air Conditioning
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IRIS	Internet Registry Information Service
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
LDAP	Lightweight Directory Access Protocol
LERG™	Telcordia Local Exchange Routing Guide
NANP	North American Numbering Plan
NAPTR	Naming Authority Pointer (DNS Resource Record)
NIC	Network Information Center
NPA	Numbering Plan Area
NPAC	Number Portability Administration Center
NS	Name Server
OAM&P	Operations Administration Maintenance and Provisioning
PoP	Point of Presence
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre

RRs	Resource Record
RTT	Round-Trip Time
SP	Service Provider
SPR	Service Provider of Record
SRS	Shared Registration System
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
TN	Telephone Number
TSIG	Transaction Signatures
TSP	Telephony Service Provider
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	Unicode Transformation Format -8 encoding
US	United States of America
WWW	World Wide Web

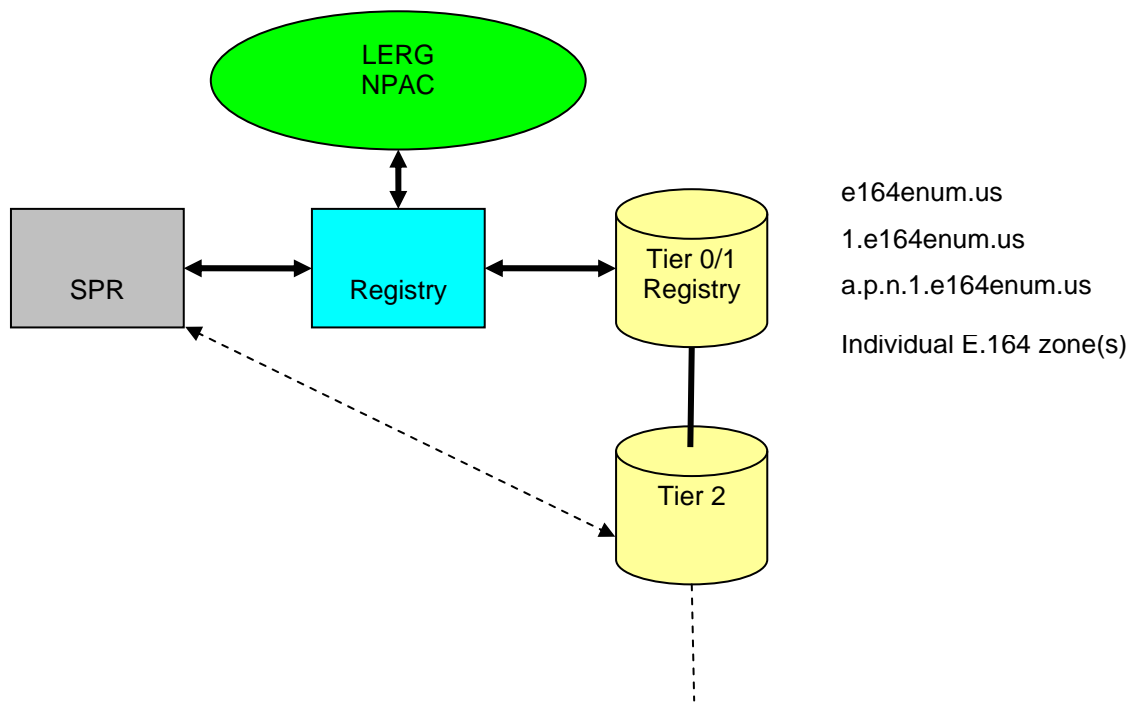
▪ SECTION 4.0 INTRODUCTION

This section specifies the reference architecture of a single common ENUM DNS domain, nominally e164enum.us, within the United States, and potentially other Country Code 1 nations that choose to participate. The plan of the CC1 ENUM LLC is to implement Provider ENUM in a separate domain from User ENUM, specific to the US or Country Code 1. When a global apex is established for Provider ENUM, it is the intent of the LLC to merge the US/CC1 implementation into the global tree.<sup>2</sup>

Accordingly, a tiered architecture parallel to the User ENUM implementation in 1.e164.arpa is presented as the target but initial implementation will consist of a collapsed Tier 0/1.

**4.1 Interim Implementation**

The initial Provider ENUM implementation is based on a collapsed tiered architecture as shown in Figure 1. The combined Tier 0/1 Registry would host e164enum.us and 1.e164enum.us domains, with entries in the 1.e164enum.us zone corresponding to US NPAs as well as containing the NS records for individual numbers within those NPAs. The remainder of this document will discuss requirements in terms of the initial architecture but except where noted, requirements apply to all phases of implementation.



**FIGURE 1 – Interim Provider ENUM Functional Architecture**

<sup>2</sup> ie164.arpa has been proposed in the IETF as a potential global root for Provider ENUM.

Service Providers of Record, the entities that register numbers into the Provider ENUM Tier 0/1 Registry, will, in turn, be required to establish a business relationship with the CC1 ENUM Tier 0/1 Provider ENUM Registry Operator prior to registering any telephone number in e164enum.us.

The nature of the business relationship between the Tier 0/1 and the SPR will be defined by the LLC, embodied in a Registry agreement, and will be the same for all SPRs entered into Tier 0/1. Entries in the Tier 0/1 name servers point to the name servers of the Tier 2 provider for a given E.164 number. The Tier 2 Provider for an E.164 number maintains the actual NAPTR records that contain URIs for specific communication services, and these records are used to support interconnection between service providers.

If other NANP nations elect to join with the US in implementing Provider ENUM under e164enum.us, their NPAs and numbers could be added to the Tier 0/1, or, if they prefer to maintain a separate registry, their NPAs could be delegated to that registry from the US Tier 0/1.

In any case, the LLC seeks integration with other national Provider ENUM trees as they are deployed rather than waiting until the development of a global tree subject to agreements with the corresponding registry operators. This will be achieved through the population of DNAME records for the corresponding country codes under e164enum.us. These records would point to the apex domain of the other national tree. Likewise DNAME records for country code 1 (or country code 1 NPAs if NANP consensus is not achieved) would be populated in the other national trees pointing to e164enum.us.

It is anticipated that SPRs will generally be Tier 2 providers for their numbers though they may elect to outsource this function to other entities. It is also anticipated that SPRs will want to provide different interconnection points to different interconnection partners. A variety of techniques exist to accomplish this, resulting in either a differential response from Tier 2 or differential resolution by different interconnection partners of a common Tier 2 response. These considerations are not expected affect the Tier 0/1 functionality that is the focus of this document.

## 4.2 Target Implementation

Target Provider ENUM implementation is based on a tiered architecture as shown in Figure 2. At Tier 0 is the ie164.arpa zone.<sup>3</sup> Entries in Tier 0 name servers correspond to country codes and point to the name servers of the Tier 1 Registry that is the authoritative name server for that country code. Entries in Tier 1 Registries normally correspond to individual telephone numbers and point to the Tier 2 name servers that hold the NAPTR records used to provide actual communication services.

Because Country Code 1 corresponds to an integrated numbering plan in which the country code is shared among several countries, the plan of the LLC is to split Tier 1 functionality into a Tier 1A, which would receive the CC1 delegation from the Tier 0, and potentially multiple Tier 1Bs serving different CC1 (NANP) member countries. Entries in Tier 1 A will correspond to NPAs and will point to the Tier 1B that holds per –number delegations for the numbers within the given NPA.

Tier 1 B Registries are required to deal directly with the CC1 ENUM Tier 1A Registry to arrange for the provisioning of NS records for the NPAs they serve into the CC1 ENUM Tier 1A Registry.

CC1 ENUM Tier1B Registry(ies) will be required to establish a business relationship with the CC1 ENUM Tier 1A Registry prior to registering any NPA in ie164.arpa. The nature of the business relationship will be defined by the CC1 ENUM LLC, embodied in a Registry agreement, and will be the same for all CC1 ENUM Tier1B Registry(ies). This is necessary to ensure that each CC1 ENUM Tier1B Registry's records are properly maintained and that only the assignee of the NPA which has been designated to participate in ENUM by the national administration in charge of the NPA in question can register it into Tier 1A. The Tier 1B Registry Operator is responsible for verifying that the numbers an SPR seeks to register are served by the SPR based on the LERG and NPAC.

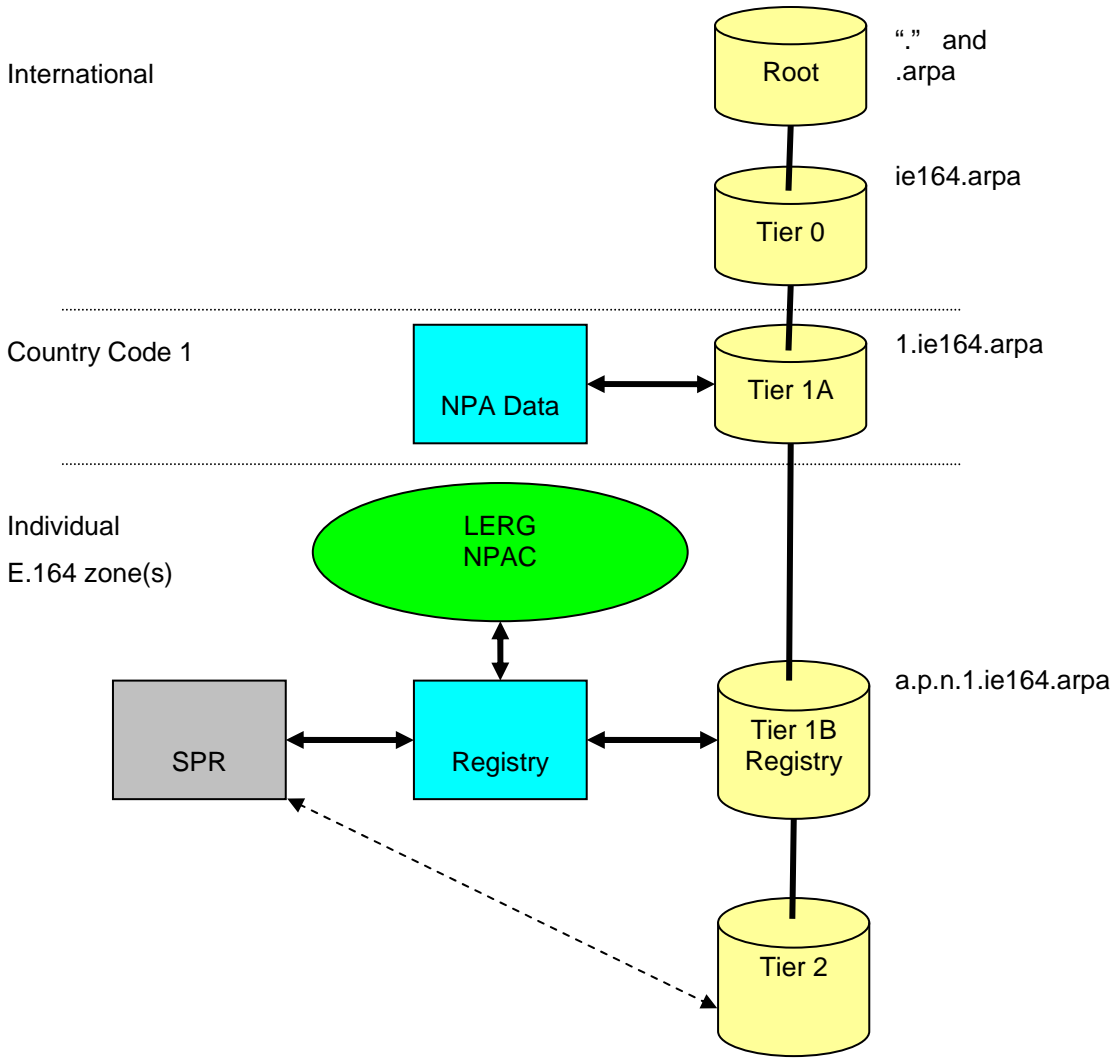
Service Providers of Record, the entities that register numbers into the Provider ENUM Tier 1B Registry Operator, will, in turn, be required to establish a business relationship with the CC1 ENUM Tier1B Provider Registry Operator prior to registering any telephone number in ie164.arpa.

The nature of the business relationship between the Tier 1B and the SPR will be defined by the LLC, embodied in a Registry agreement, and will be the same for all SPRs for a given NPA entered into Tier 1A. Entries in the Tier 1B name servers point to the name servers of the Tier 2 provider for a given E.164 number. The Tier 2 Provider for an E.164 number maintains the actual NAPTR records that contain URIs for specific communication services, and these records are used to support interconnection between service providers.

---

<sup>3</sup> For user ENUM RIPE NCC provides the Tier 0 function. The instructions regarding operations of the domain e164.arpa can be found at the URL: <http://www.ripe.net/rs/enum/instructions.html> . It is presumed that instantiation of a global Provider ENUM will result in a parallel process for the chosen domain with a to be determined operator. For illustrative purposes this document uses the domain ie164.arpa.

The ITU-T TSB evaluates e164.arpa delegation requests. Information on how TSB will handle ENUM requests can be found under the bullet "Interim Procedures" at the ITU-T Web site at: <http://www.itu.int/ITU-T/inr/enum/>.



**FIGURE 2 –Provider ENUM Functional Architecture**

## ▪ SECTION 5.0 OPERATIONAL & INFRASTRUCTURE REQUIREMENTS

---

This section provides requirements for the operation and infrastructure of the ENUM Tier 0/1 Registry. Service Level Requirements are contained in Section 6.0.

### 5.1 Registry Database

The Registry database is the central repository for all objects concerning ENUM domain name registrations in an ENUM Tier 0/1 Registry. The three primary objects associated with an ENUM Tier 0/1 registration are: domain, host, and contact. It is critical that a Registry database operate in a responsive and robust manner.

An ENUM Tier 0/1 Registry bidder should describe how it would meet the following requirements for an ENUM Registry database, and it should provide estimates of demand if necessary. (See Service Level Requirements (SLR) Section)

An ENUM Tier 0/1 Registry shall follow the “thick registry” model as detailed in Section 5.4 below. A Registry database:

- Shall be sized to accommodate the expected demand at initial launch, and to support growth without interruption as Provider ENUM matures.
- Shall be able to perform transactions at a rate that meets the needs of the ENUM users.
- Shall maintain its performance based on agreed to service-level measurements, even as the number of users, workload volume, or database size increases.
- Shall maintain a high level of availability as required by the Service Level Requirements (SLRs) contained herein. An ENUM Tier 0/1 Registry bidder should describe what level of availability it believes is necessary, what amount of scheduled maintenance is necessary, and how it would expect to meet the appropriate availability level.
- Shall be replicated and hosted in geographically dispersed data centers to achieve high availability and facilitate data backup and recovery.

### 5.2 Shared Registration System (SRS)

The Tier 0/1 Registry Operator shall provide a Shared Registration System (SRS) that allows multiple Service Providers of Record to enter ENUM registrations into the registry. An ENUM Tier 0/1 Registry will maintain the addresses of the name servers of the Tier 2 providers in the US ENUM name space and will have authority to communicate with the ENUM Tier 1A Registry when and if the target architecture is implemented.

An ENUM Tier 0/1 Registry is required to:

- Allow concurrent operations from multiple SPRs
- Verify that a number which an SPR seeks to register is allocated/porting to that SPR using data from the LERG and NPAC
- Using data from the NPAC remove registrations for numbers that have ported away from an SPR and, optionally, by agreement with the recipient SPR, establish a new registration for the number.
- Provide non-discriminatory services to each authorized SPR to perform registration related operations
- Provide and conduct non-discriminatory SPR certification procedures

- Support open standard interfaces between the ENUM Tier 0/1 Registry and authorized SPRs
- Perform Zone data creation and maintenance necessary to update the zone data and information in the local data stores (see Section 5.3)
- Support open standard interface(s)

### 5.3 *Zone Data*

Zone data is typically a database file (or a collection of database files) consisting of the technical information that the DNS requires to function correctly. Zone data generation is the term traditionally used to describe the process of generating zone information from the Registry database, deploying it to the primary server, and then propagating it out to the secondary servers. The latter two steps are also called zone data propagation.

An ENUM Tier 0/1 Registry bidder must describe how it would meet the following requirements for zone data operations:

- The SRS/Registry Database shall provide means to generate the zone data from the Registry database to reflect changes made through the ENUM Registry- Service Provider of Record interface as defined in the Service Level Requirements (SLRs in Section 6.)
- The zone data, once generated by SRS/Registry Database, shall be reliably and securely propagated to all ENUM Tier 0/1 name servers with minimum delay.
- The frequency of zone data generation and the delay of zone data propagation shall meet the SLR requirements
- Zone data generation and propagation procedures shall be carefully engineered so that they will not adversely affect the normal ENUM Tier 0/1 Registry and name server operations.
- Zone data distribution procedure should conform to appropriate IETF standards (see Section 2)
- The SPR to ENUM Tier 0/1 Registry SRS shall be the only automatic means by which a SPR can make changes to its ENUM domain names without the need for Registry personnel intervention.
- The name servers for an ENUM Tier 0/1 Registry shall be placed in geographically dispersed data centers topically diverse connections to the Internet to allow for maximum redundancy against disaster and failures.
- The registry database shall support logging and backup capabilities for all zone data updates.

### 5.4 *Thick Registry Model*

A thick registry is one in which all of the information associated with registered entities, including both technical information (information needed to produce zone files) and social information (information needed to implement operational, business, or legal practices), is stored within a central registry repository. To protect the privacy of Service Provider of Record information, public access to the thick registry will be limited. Details for access to registration data are found in Section 5.5.

It is understood that technical information populated into the Tier 0/1 Registry DNS resource records is intended to be publicly available for responses to DNS queries.

### 5.5 *ContactInfo*

Instead of a conventional WHOIS service, a new query service known as ContactInfo will be provided for ENUM. This service will provide a means of contacting the SPR for trouble resolution. It will also allow for appropriate disclosure of SPR information for authorized law enforcement inquiries. An ENUM Tier 0/1 Registry bidder is required to describe how they would provide this service to meet the needs of the

communications industry while safeguarding the non-public information of SPRs from a technical perspective. The Tier 0/1 operator will respond to all lawful ContactInfo requests from appropriate authorities.

ContactInfo may also be used to support other industry functions, e.g., associating a service type with a number (i.e., VoIP) per OBF request.

### **5.5.1 Introduction**

This section describes specific requirements for the Tier 0/1 operator to maintain a ‘ContactInfo’ database. Also included in this section are the following: how the database should be operated, and what information should be publicly accessible.

### **5.5.2 Need for ContactInfo Databases**

1. There is a need for the Tier 0/1 Operator to maintain ContactInfo databases associated with ENUM registrations.
2. The appropriate technology for maintaining public access to such ContactInfo should be the IRIS protocol developed by the CRISP Working Group.
3. There is a requirement on the Tier 0/1 operator to maintain such a database in a manner known as the “Thick Registry” where the Tier 0/1 Operator maintains the authoritative database of registration information obtained from all SPRs.
4. The information from that database that could be made accessible to which parties is a matter of policy for the CC1 ENUM LLC to determine, to ensure compliance with privacy regulations and best practices.

### **5.5.3 General ContactInfo Requirements**

The general requirements for the ContactInfo database are:

1. Mining Prevention: providing some technical means to discourage data mining of the information base
2. Standard and Extensible Schemas
3. Level of access: not all data need be equally accessible by all users of the service
4. Client processing: facilitating the creation of client software that can automatically extract relevant details from the services responses
5. Searches: The protocol should provide for flexible access by authorized entities while limiting other queries to searches by full telephone number only.
6. Result Set Limits: the protocol must include provisions for allowing a server operator to express a client search limit

The implementation of ContactInfo Databases must be policy neutral and extensible to allow the LLC to administer associated ContactInfo policies, with regard to individual database elements as well as the database as a whole.

Contact-Info Databases should use modern authentication and authorization methods to control access by Registry personnel, SPRs, and querying parties.

### **5.5.4 Data Collection Requirements and ContactInfo Data Access**

ENUM accredited SPRs will transmit copies of specified data for each registration to the Tier 0/1 operator for maintenance under the concept of a “thick Registry”.

The Tier 0/1 operator will then take portions of the data, such as SPR contact data, and populate an IRIS database with that information for public access. The data that is to be publicly accessible is a matter to be governed by appropriate regulatory requirements and the Tier 0/1 contract.

Below, are the recommended data elements that should be included in the Zone ContactInfo.

The data elements that are marked as public should be made available to all queries under the terms and conditions of the Tier 0/1 contact and in compliance with appropriate regulatory requirements. All data in the database must be true and accurate. The use of proxied data is not allowed.

#### 5.5.4.1 Zone Contact Data Elements

**Table 1** Zone Contact Data Elements

<b>Data Element</b>	<b>Example</b>
Domain Name	4.5.6.7.5.5.5.3.2.1.1.e164enum.us
Domain ID	
Remarks	Service Type = VoIP
Domain Status	SPR-LOCK
Domain Updated Date	
Domain Expiration Date	
SPR Name	
SPR URL	
Last Updated by Service Provider of Record	
Last Transferred	
Name Server ID	
Name Server Name	BAY-W2.ACME.FOO
Name Server URL	Iris:ereg1//t1b.us/host/bay-w2.acme.foo
Name Server Status	
Name Server Association Status	
Name Server IP Address	
Name Server Creation Date	
Name Server Last Transfer Date	
Tier 0/1 Name	
Tier 0/1 URL	
Tier 0/1 Name Server Name	

Below are the recommended data elements that should be included in the SPR ContactInfo. The data elements that are marked as public must be made available to all queries. The data elements that are marked as private must be secured in the ContactInfo database and only available to queries that have the

appropriate authorization. The SPR has the right to change the default data elements that are marked as private to public at their discretion. If a data element is marked optional, then there is no requirement for populating those fields. These fields should be populated with role-based information (e.g., email address abuse@xyz.com)

#### 5.5.4.2 SPR Contact Data Elements

**Table 2 SPR Contact Data Elements**

<b>Data Element</b>	<b>Private</b>	<b>Public</b>	<b>Example</b>
Service Provider of Record Name		X	
Service Provider of Record Address		X	
Service Provider of Record Phone Number		X	
Service Provider of Record URL		X	
Service Provider of Record Admin. Contact Name		X	
Service Provider of Record Admin Contact Phone Number		X	
Service Provider of Record Admin Contact Email		X	

## 5.6 Security

The Tier 0/1 Registry Operator must secure both Registry operations and data. The Registry Operator shall conduct comprehensive threat analyses on all parts of the Registry system to identify the vulnerable points and the types of security attacks. Based on the analyses, the Registry Operator shall define and implement multi-tiered procedures that provide security protections to all parts of the Registry system.

The Registry Operator is required to protect Registry system access from all forms of abuse, fraud, or security breaches. In addition, a Tier 0/1 must follow any and all commercial practices used to protect credit card information (Gramm-Leach-Bliley Act).

### 5.6.1 Operational System Security

Security requirements are detailed below:

- Protection/Prevention of compromise of the systems hosting or managing Tier 0/1
- Protection from Denial of Service attacks (internal & external)
- Requirements for maintaining security updates for all software
- Security (integrity, authenticity) of communications between the components of the Tier 0/1 service (name servers, registry, etc)
- Encryption requirements
- Authentication & Authorization requirements
- Requirements on ISPs providing connectivity for Tier 0/1

### **5.6.2 Physical Security**

- The Tier 0/1 Registry Operator shall employ a variety of physical security systems to ensure that unauthorized personnel have no access to sensitive equipment and/or data.
- All servers containing any sensitive data shall be physically secured so that only a controlled list of people can obtain access.
- The hosting centers shall be secured so that no access to the internal networks is possible for unauthorized persons. All internal networks shall be isolated from public access, and external Internet links shall be firewall-protected to prevent intruders from gaining access.
- Physical precautions inside the server rooms shall include movement detectors (using infra-red or similar means) to alert security personnel should an intruder gain access to a secured location. Alarms will be fitted to all doors and windows, which open into or out of a restricted area.
- The doors and windows shall be secure enough to withstand a reasonable amount of force, and damage to doors or windows shall also trigger the alarms.
- Security staff shall be present at all times, and should have sufficient training to enable them to correct most problems. Appropriate personnel shall also be contacted when necessary to help contain the situation. (Bidder should provide its proposed escalation procedures.)
- Access to the server room shall be controlled by a two-factor authentication system. An authorized individual shall require both an authorized access token and a valid PIN or passcode to gain physical access to the servers. Any use of an access token shall be logged and such logs shall be archived for at least 1 year.
- Should an access card be lost or stolen, it is the responsibility of each employee to report this in a timely manner so that the lost card may be deactivated and a new card issued. Closed circuit TV shall be in place at all sites for identification purposes should an unauthorized person attempt to use a stolen access card. Personnel authorized temporary access to the servers, but not permanently issued access tokens, shall be escorted by permanent staff while within the restricted space.
- 24-hour access to the data center by authorized personnel shall not be hindered by aforesaid security measures.

### **5.6.3 Network Security**

- The Tier 0/1 shall use techniques such as User identification, passwords, and/or IP range checking for all restricted services (which includes services other than DNS resolution.).
- Secure File Transfer Protocols shall be used for all "file transfers" between the ENUM Tier 0/1s and the Tier 1A Registry [RFC 2228, RFC 2577, or similar equivalent] when and if the target architecture is implemented.
- System maintenance shall be performed via SSL or similarly secured connections. Telnet servers shall not be operational on any system on the DNS network due to their security risk.
- Each system shall operate a very restricted set of basic services in the relevant sections for DNS, ContactInfo, FTP, SCP, and WWW services. Systems shall be firewall-protected in hardware, and IP filtering rule sets shall be in place to reject packets that are not appropriate for a particular host.
- DNS servers shall run a minimum set of applications and system services, in addition to the DNS server software.

- The Tier 0/1 Operator shall check all its DNS servers to ensure that data integrity is maintained.
- Services which are IP-restricted shall have each IP address specified individually. Network addresses are not to be used, since this adds the risk that a host could masquerade as a spare IP address on an internal network.
- Packet "sniffers", designed to check all traffic passing through a network interface, shall be in place to catch suspicious traffic. These will actively scan for incorrect or illegal packets, and alert the security team. Packet sniffers may also give some indication of the source of an attack, which would be of use in preventing that attack in the future.
- Network security shall be verified by a security audit process, which involves scanning from an internet-connected host all TCP and UDP ports on servers operated by the Tier 0/1 Registry.
- Security tests shall be performed on the DNS Servers and a corresponding report audited on a regular basis. Each test will attempt to take advantage of a security flaw using a specific attack method, and the result shall be reported. Here is a non-exhaustive list of known attacks:
  - Buffer overflow exploit
  - Missing format string exploit
  - Packet fragmentation attack
  - Data flooding (SMURF ping, etc.)
  - DNS spoofing
  - FTP spoofing
  - Dictionary passwords
  - Replay attack
  - Denial of service (DoS)

Some of these attacks may not be applicable to all services.

The Tier 0/1 Registry Operator shall update the tests used when new vulnerabilities, security flaws, or techniques are discovered. The updates shall be based on information from security-related mailing lists, websites, newsgroups, and industry best practices.

#### **5.6.4 Backup Security**

- Backup shall be performed in a secure manner on the main Tier 0/1 Registry site.
- The Tier 0/1 Registry Operator shall use an encryption scheme for the backup of sensitive data as a part of the implementation process.
- Backup information shall be stored in a secure off-site location.

#### **5.6.5 Security Audit and Reporting**

The Tier 0/1 Registry Operator shall run a security audit on a regular basis but no less often than once per quarter.

- The Tier 0/1 Registry Operator shall run a security audit to test all systems for configuration issues and security vulnerabilities. Results of this audit should then form the basis of a quarterly security audit report, which will also detail any recommendations for system alterations and a timeline for remediation.
- All security breaches are to be reported to the Registry management responsible for security and to the CC1 ENUM LLC. Should a serious breach be detected, some services may be suspended temporarily if this is necessary to ensure the reliability of the Tier 0/1 Registry data. Bidders should detail the hierarchy of breach severity and escalation procedures.
- The Tier 0/1 Registry Operator shall provide a monthly security status report to the CC1 ENUM LLC, including a list of security incidents categorized by severity.

### **5.6.6 Resolution Access Control**

Although it is the intent of the LLC to make the initial AoR for an ENUM registration publicly accessible, regulatory constraints may ultimately result in the need to restrict access to name resolution services to SPRs and other qualified parties pursuant to a user agreement. Bidders should offer proposals on how best to implement such controls<sup>4</sup>.

### **5.7 Caching Requirements**

This section refers to the minimum requirements for caching. Bidders should propose what they believe are appropriate values for name server caching requirements for time to live (TTL).

### **5.8 System Turn-Up and Testing**

Bidders need to provide a detailed start-up project implementation and system test plan, including proposed test cases, to support the Tier 0/1 registry system turn-up.

A Beta test period is recommended as a critical final step prior to successful commercial deployment. The Bidder should propose an appropriate plan and set of parameters for Beta testing.

Bidders are required to provide high level start-up project implementation timelines and plans as part of their bid proposal.

### **5.9 Operations and Maintenance**

ENUM is envisioned as a wholly robust and high-availability service. An ENUM Tier 0/1 Registry bidder should describe how it would operate and maintain the various aspects of the Registry at a high service level. Bidders should include descriptions of how they intend to ensure system reliability, system recovery procedures, and technical support, including arrangements for power, HVAC (Heating, Ventilating, and Air Conditioning), and fire systems.

An ENUM Tier 0/1 Registry bidder should also provide a comprehensive description of how they will manage their network operations center to address the following:

- Trouble reporting and ticket tracking:
  - How Tier 2 Providers and SPRs can submit trouble tickets and receive status reports.
  - Tracking of internal performance metrics.
- Technician support 24x7x365:
  - Internal hand off between different technician levels (1, 2, etc).
  - Internal hand off between different support groups.
  - Trouble referral and tracking to third party entities.
- Monitoring of servers and network connections

---

<sup>4</sup> Such controls would complicate the ability to provide international interoperability.

- Intrusion detection for both physical and network security
- Provide technical liaison with the Tier 1A entity for issues related to delegation authority over NPAs within 1.1e164.arpa if and when the target architecture is implemented.
- Provide a description on how escalations will be handled and communicated to the Tier 2 and SPRs.
- Describe disaster recovery plans to restore critical components of the system within 48 hours in the case of a force majeure event. No single event should result in an outage of DNS resolution service itself.
- Describe how the network operations center will perform internal monitoring as a means to verify that the availability and performance measurements in this document are being met and provide reports on a monthly basis to the CC1 ENUM LLC or its designee.
- Describe information retention practice to ensure that the summary data is kept for the life of the contract and that valid ticket data is kept on a rolling thirteen-month basis in the trouble reporting system.

## 5.10 System Recovery Procedures

System recovery refers to the process of bringing the system back to normal operations after the system has gone down due to failures. The goal is to minimize downtime, data loss, and adverse impacts on other systems.

- In describing how it intends should meet operations and maintenance requirements the ENUM Tier 0/1 Registry bidder should: Specify how it will employ recovery procedures for failures that occur at different parts of the Registry system, such as:
  - Data center failures
  - Database failures
  - Server failures
  - Network failures
- Specify how redundancy and highly available Registry architecture will help expedite recovery from these failures.
- Specify how backup and escrow data will be used for recovery from these failures.

In addition the bidder should describe how it would:

- Provide a time estimate for recovering from each type of failure.
- Log each system outage and document system problems that could result in outages.

## 5.11 Database Escrow and Backup

The goal of any data backup/recovery procedure is full and timely recovery from failures without any loss of data. Data backup strategies handle system hardware failures (e.g., loss of a processor or one or more disk drives) by reinstalling the data from daily backups, supplemented by the information on the “before” and “after” backup files that the database creates. In order to guard against loss of the entire facility because of fire, flood, or other natural or man-made disaster, off-site escrow of the Registry data should be provided in a secured storage facility.

An ENUM Tier 0/1 Registry bidder shall specify:

- The frequency and procedures for data backup

- The frequency and procedures for data escrow
- The hardware and software systems used for data backup
- The procedures for retrieval of data and rebuild of the database
- Who should have access to the escrowed data and in what circumstances it would be accessed by an entity other than itself
- Testing process and schedule to verify the escrow and database backup procedure
- The data escrow arrangements, including any contractual arrangements with Third parties

In addition, the following safeguards are required of ENUM Tier 0/1 Registry bidders:

- The data backup and escrow procedures shall not impede the overall performance of normal Registry operations
- The data backup and recovery procedures shall minimize the data loss and service interruption of the Registry

### **5.12 Technical and Other Support**

The Tier 0/1 Registry Operator must provide technical and other support to SPRs and Tier 2 providers from an appropriate customer help desk with a well-defined escalation policy.

The Registry Operator must work with other national Provider ENUM Registries to implement and support linking of the corresponding Provider ENUM trees as directed by the LLC.

In the initial interim implementation the Registry Operator may also need to support Tier 1Bs of other NANP nations that choose to delegate their NPAs from the Tier 0/1 Registry under agreement with the LLC.

If and when the target architecture is implemented, the Tier 1B Registry Operator must provide technical support to the Tier 1A for resolution of issues with respect to the delegation of authority over a country's NPAs within 1.ie164.arpa.

The RFP should require the Registry bidders to describe how they would fulfill these requirements

### **5.13 Transition**

The Tier 0/1 Registry Operator must provide a plan for transitioning of the Registry to a new provider should that be required under the terms of the contract. The plan must ensure no disruption of Tier 0/1 function in providing ENUM DNS service.

### **5.14 Accommodation of Future Internet Architectural Enhancements**

Bidders must respond with plan to accommodate IPv6 per RFC 2874.

Bidders must respond with plan to accommodate DNSSEC per RFC 2535.

## ▪ SECTION 6.0 SERVICE LEVEL REQUIREMENTS (SLR)

---

The Tier 0/1 Registry Operator shall use commercially reasonable efforts to provide performance at the levels set forth herein.

### 6.1 Service Availability

Service Availability is measured as follows:

Service Availability % =  $\{[(MTM - POMU) - UOM] / (MTM - POMU)\} * 100$  where:

MTM = Monthly Timeframe Minutes calculated as the number days in that month times 24 hours times 60 minutes. For example, the MTM for January is 31 days \* 24 hours \* 60 minutes or MTM = 44,640 minutes.

POMU = Planned Outage Minutes Used is the number of minutes of a Planned Outage or Extended Planned Outage Used for that Monthly Timeframe for each individual System Service. No Monthly Timeframe shall have both a Planned and an Extended Planned Outage.

UOM = Unplanned Outage Minutes

#### 6.1.1 DNS Resolution Service

The Service Availability calculation shall be calculated by the Registry Operator and the results reported for each Monthly Timeframe for DNS Name Server availability. Results will be reported to the SPR Community via e-mail and to CC1 ENUM LLC.

Service Availability--DNS Name Service = 100% per calendar month. Service Availability as it applies to the DNS Name Server refers to the ability of the DNS Name Server to resolve a DNS query from an Internet user. DNS Name Service unavailability will be logged with the Registry Operator as Unplanned Outage Minutes. Registry Operator will log DNS Name Service unavailability when such unavailability is detected by monitoring tools, or once an SPR reports an occurrence to Registry Operator's customer service help desk in the manner required by the Registry Operator (i.e., e-mail, fax, and telephone) and Registry Operator confirms that the occurrence is not unique to the reporting SPR. DNS Name Service unavailability shall mean when greater than 25% of sites on the Registry Operator's constellation are returning answers to queries with more than 1% packet loss averaged over a Monthly Timeframe or 5% packet loss for any five minute period. The committed Service Availability for DNS Name Server is 100% per calendar year.

Planned Outage – For DNS resolution service no Planned Outages are allowed

#### 6.1.2 SRS

Service Availability as it applies to the SRS refers to the ability of the SRS to respond to SPRs that access and use the SRS through the EPP or designated protocol. SRS Unavailability will be logged with the Registry Operator as Unplanned Outage Minutes. The committed Service Availability for SRS is 99.95% and the Service Level Measurement Period is monthly.

- **SRS Planned Outage Duration = 45 minutes per Monthly Timeframe**
- **SRS Planned Outage Timeframe = 0600-1400 UTC Sunday**
- **SRS General Maintenance Planned Outage notification Timeframe = 30 days**
- **SRS Updates/Upgrades notification timeframe = 90 days**  
(as defined in the Patch, Update and Upgrade Policy)

### 6.1.3 *ContactInfo*

Service Availability as it applies to ContactInfo refers to the ability of users to access and use the Registry's ContactInfo service. ContactInfo Unavailability will be logged with the Registry Operator as Unplanned Outage Minutes. The committed Service Availability for ContactInfo is 99.95% and the Service Level Measurement Period is monthly.

- **ContactInfo Planned Outage Duration = 45 minutes per Monthly Timeframe**
- **ContactInfo Outage Timeframe = 0600-1400 UTC Sunday**
- **ContactInfo Maintenance Planned Outage Notification Timeframe = 30 days**
- **ContactInfo Updates/Upgrades notification timeframe = 90 days**  
(as defined in the Patch, Update and Upgrade Policy)

## 6.2 **Processing Time**

Processing time is an important measurement of transaction-based services like the System Services. Service Availability, including Planned Outages and Extended Planned Outages, measures the amount of time that the service is available to its users. Processing time measures the quality of Service Availability.

Processing Time refers to the round-trip for the System Services ("Processing Time"). Since each of the System Services has a unique function, the Performance Specifications Processing Times are unique to each System Service. Processing Time Performance Specifications will be measured in a monthly timeframe and will be reported on a monthly basis to the CC1 ENUM LLC.

### 6.2.1 *DNS Resolution Service*

Processing Time--DNS Name Server Resolution  $\leq$  100 milliseconds for 95%. Bidders should provide sufficient detailed justification for any proposal that does not meet this requirement.

- a) Processing Time - DNS Name Server Resolution is applicable to the DNS Name Server. It measures the processing time for a DNS query.
- b) The Performance Specification is 100 milliseconds for 95% of the transactions. That is, 95% of the transactions during a Monthly Timeframe will take 100 milliseconds or less from the time name server receives the DNS query to the time it provides a response.

### 6.2.2 *SRS*

#### 1. **Processing Time Add, Modify, Delete = 1000 milliseconds for 95%.**

- Processing Time - Add, Modify, and Delete is applicable to the SRS as accessed through the EPP protocol defined in Appendix C. It measures the processing time for add, modify, and delete transactions associated with domain names, name servers, contacts, and SPR profile information.
- The Performance Specification is 1000 milliseconds for 95% of the transactions processed. That is, 95% of the transactions will take 1000 millisecond or less from the time the Registry Operator receives the request to the time it provides a response.

#### 2. **Processing Time--Query Domain**

- ContactInfo Processing Time - Query Domain is applicable to the SRS as accessed through the designated protocol. It measures the processing time for an availability query of a specific domain name.
- The performance specification is 500 milliseconds for 95% of the transactions. That is, 95% of the transactions will take 500 milliseconds or less from the time the Registry Operator receives the query to the time it provides a response as to the domain name's availability.

### 6.2.3 *ContactInfo*

- Processing Time - ContactInfo Query is only applicable to the ContactInfo. It measures the processing time for a ContactInfo Query.
- The Performance Specification is 1000 milliseconds for 95% of the transactions. That is, 95% of the transactions will take 1000 milliseconds or less from the time the ContactInfo receives a query to the time it responds.

## 6.3 Update Frequency

There are two important elements of the Registry that are updated frequently and are used by SPRs; Name server and ContactInfo. SPRs generate these updates through the SRS. The SRS then updates the Name server and the ContactInfo. These will be done on a batch basis.

The committed Performance Specification with regard to Update Frequency for both the Name server and the ContactInfo is 10 minutes for 95% of the transactions. That is, 95% of the updates to the Name server and ContactInfo will be effectuated within 10 minutes. This is measured from the time that the registry confirms the update to the SPR to the time the update appears in the name servers and ContactInfo.

Update Frequency Performance Specifications have a monthly Service Level Measurement Period and will be reported on a monthly basis.

- Update Frequency--Name Server = 10 minutes for 95%.
- Update Frequency-- ContactInfo = 10 minutes for 95%.

## 6.4 Cross-Network Name Server Performance (CNNP)

DNS Name Server Round-trip and packet loss from the Internet are important elements of the quality of service provided by the Registry Operator. These characteristics, however, are affected by Internet performance and, therefore, cannot be closely controlled by Registry Operator. The committed performance specification for cross-network name server performance is a measured Round-trip of fewer than 300 milliseconds and measured packet loss of under 1% averaged over the course of a Monthly Timeframe and no greater than 5% for any five (5) minute period over the course of a Monthly Timeframe. Cross-network name server performance measurements may be conducted by the CC1 ENUM LLC at times of its choosing, in the following manner:

- 1) The measurements will be conducted by sending strings of DNS request packets from each of four measuring locations to each of the Tier 0/1's DNS Name Servers and observing the responses from the Tier 0/1's DNS Name Servers. (These strings of requests and responses are referred to as a "CNNP Test".) The measuring locations should be at least four geographically diverse sites.
- 2) Each string of request packets will consist of 100 UDP packets at 10-second intervals requesting name server (NS) records for arbitrarily selected Tier 0/1 domains, pre-selected to ensure that the NPAs exist in the Registry and are resolvable. The packet loss (i.e. the percentage of response packets not received) and the average round-trip time for response packets received will be recorded.
- 3) To meet the packet loss and Round-trip requirements for a particular CNNP Test, all three of the following must be true:
  - a) The Round-trip and packet loss from each measurement location to at least one Tier 0/1 name server must not exceed the required values.

- b) The packet loss to each of the Tier 0/1 name servers from at least one of the measurement locations must not exceed the required value.
- c) The Round-trip time to each of 75% of the Name servers from at least one of the measurement locations must not exceed the required value.
- 4) Any failing CNNP Test result obtained during an identified Core Internet Service Failure shall not be considered. "Core Internet Service Failure" refers to an extraordinary and identifiable event beyond the control of Registry Operator affecting the Internet services to be measured. Such events include but are not limited to congestion collapse, partitioning, power grid failures, and routing failures.
- 5) To ensure a properly diverse testing sample, the testing entity will conduct the CNNP Tests at varying times (i.e. at different times of the day, as well as on different days of the week).
- 6) In the event of persistent failure of the CNNP Tests (three or more consecutive failed tests), CC1 ENUM LLC will give Registry Operator written notice of the failures (with backup data) and Registry Operator will have sixty days to cure the failure.
- 7) Sixty days prior to the commencement of testing under this provision, CC1 ENUM LLC will provide Registry Operator with the opportunity to evaluate the testing tools and procedures to be used by testing entity. In the event that Registry Operator does not approve of such tools and procedures, the testing entity will work directly with Registry Operator to make necessary modifications.

## **6.5 Internet Connectivity**

Bidders must describe the physical connectivity arrangements planned to support each of their name servers and how these arrangements will enhance service reliability and security.

## **6.6 Shared Registration System (SRS)**

An ENUM Tier 0/1 Registry bidder shall propose service-level requirements it would expect to meet with regard to operations of the SRS. This shall include the following items:

- Registry database throughput – number of transactions per second
- Registry database availability (in line with 6.1.2)
- Number of ENUM Service Provider of Record accounts
- Number of concurrent ENUM SPR -ENUM Registry connections
- Frequency of zone data generation: rates per day, hour, minute

## **6.7 Reports and Files**

An ENUM Tier 0/1 Registry Operator shall provide reporting service to Service Providers of Record and the LLC. In addition, it may make zone data available to Service Providers of Record and other contracting entities under terms and conditions established by the LLC restricting the use of such data to network uses and not for marketing purposes. The bidder should propose the types and frequency of reports it will provide to both the SPRs and the LLC.

Details of information to be included in reports are provided in section 10.

Except in the case of Name Server performance requirements, the Tier 0/1 Registry Operator will perform internal monitoring as a means to verify that the availability and performance measurements of this document are being met.

Beginning no later than 120 days after the commencement-of-service date, the ENUM Tier 0/1 Registry Operator will provide preliminary monthly system performance and availability reports to the LLC.

The ENUM Tier 0/1 Registry Operator will provide service availability percentages during each Performance Measurement Period as listed in this document.

An ENUM Tier 0/1 Registry Operator may provide custom reporting service that would allow ENUM SPR and the LLC to specify report criteria and have the report available for download upon completion.

These reports should be posted to a secure site (i.e., FTP (File Transfer Protocol)) that can be accessed by the SPRs by entering username and pass code.

The format for reports should be easily machine-readable by SPRs (i.e., XML, CSV).

Naming convention of reports should identify the SPRs, the date the report was created, and the subject of the report.

An ENUM Tier 0/1 Registry Operator should archive copies of all reports created.

An ENUM Tier 0/1 Registry bidder is required to address what mechanisms it would use to enable the contracting entity to:

- Monitor the initial progress of implementation
- Monitor the ongoing participation in the offering
- Monitor and provide feedback regarding the ongoing performance of the Tier 1
- Monitor ongoing system updates and changes
- Monitor ongoing policy updates and changes
- Drive system updates and changes
- Drive policy updates and changes

## ▪ SECTION 7.0 INTERFACE REQUIREMENTS

---

### 7.1 Interfaces between Registry and Service Provider of Record

The Tier 0/1 Registry-SPR interface will be a shared registration system (SRS) whereby accredited SPRs or their authorized agent (e.g., a service bureau) may register ENUM domain names for their numbers in the CC1 ENUM name space. The Tier 0/1 Registry Operator will be required to develop a Registry-Service Provider of Record Agreement. The Registry and Service Provider of Record Agreement will include the details regarding the interface protocols that can be used.

A Tier 0/1 Shared Registration System (SRS) is required to:

- Allow an unlimited number of SPRs to register ENUM domain names in the US Provider ENUM name space
- Provide equivalent access to the system for all SPRs to perform registration related operations such as:
  - Register new ENUM domain names and associated information
  - Check status of registered ENUM domain names and associated information,
  - Delete registered ENUM domain names and associated information,
  - Update information about registered ENUM domain names and associated information,
- Support the open standard interface between the Registry and SPR, as defined in the IETF extensible provisioning protocol (EPP) standard suite (RFC3730 through RFC3735 and RFC 4114). The Tier 0/1 Registry Operator will work with the industry to identify and develop further extensions to EPP for the purposes of supporting US Provider ENUM if needed.
- The common Tier 0/1 registry protocol for SPR shall be EPP but this should not preclude other protocols from being used between the registry and SPRs.
- Reject illegal commands/requests (e.g., missing mandatory data element) from ENUM SPR.

The bidder should propose a set of security applications for the SRS, such as what is being proposed in the following:

- Security of the SRS applications shall be provided in part via the mandatory use of the TLS [RFC 2246] protocol for transport layer security.
- Each EPP session shall be authenticated and encrypted using TLS. The ENUM Registry shall authenticate every EPP client connection using both an X.509 server certificate, issued by a commercial Certification Authority identified by the Tier 0/1 Registry, and its SPR password.
- Security of the SRS application shall be provided via an authenticated and encrypted connection. At a minimum, IPSEC will be used to secure the connection.
- Each EPP session shall be authenticated and encrypted using IPSEC. The Tier 0/1 Registry shall authenticate every EPP client connection using a valid PKI.

The Tier 0/1 must support batch file processing so that the ENUM SPR can put many commands into one file and deposit it in a “command” directory on a Tier 0/1 Registry server. The Tier 0/1 Registry Operator should move the file to an archive directory, process the commands based on the order as they appear in the file, and put all the responses to the commands in the same order in a file that is deposited in a “response” directory on the same server. ENUM SPR can periodically check and retrieve files in the “response” directory. Once the file is read, the ENUM Tier 0/1 Registry can move the file to an archive directory where it can be preserved as backup.

## **7.2 *Interfaces between Tier 1A Registry and Tier 0/1 Registry***

If and when the target architecture is implemented, the Tier 1A registry will likely contain less than a thousand records and additions and changes are expected to be infrequent. Thus, a formal mechanized interface or system (Shared Registration System) between Tier 0/1s and the Tier 1A may not be required.

## **7.3 *Other Interfaces***

- The interface between the ENUM SPR and the Tier 2 Provider, if the SPR choose to outsource that function is a matter between the parties.
- The Tier 0/1 Registry Operator must become an NPAC user and establish the appropriate interfaces to obtain NPAC data for registration validation and porting notification
- The Tier 0/1 Registry Operator must subscribe to the LERG to obtain data for registration validation

## ▪ SECTION 8.0 PROVISIONING

---

This section defines provisioning requirements and procedures for ENUM administration. This involves the following ENUM functional entities: Service Provider of Record, ENUM Tier 0/1 Registry Operator, and, potentially a Tier 2 provider if the SPR elects to outsource these functions. This section will address the tasks and responsibilities required to provision and maintain ENUM registrations by the above functional entities with the focus on the interface between the Tier 0/1 Registry and the SPR.

This section does not include procedures for interaction with the Tier 1A Registry.

### **8.1 Assumptions**

The following assumptions are made when describing the provisioning scenarios:

- SPRs will be bound by a Registry agreement developed by the Tier 0/1 Registry Operator together with the LLC. This agreement will require the SPR to comply with the procedures detailed below. In addition to the provisioning procedures, the Registry agreement will detail data privacy requirements. SPRs have an established trust relationship with the Tier 0/1 Registry. This relationship includes the method for secure communication, user authentication (e.g., the assignment of a user identification (ID) and password for session management), a SPR ID for ENUM Registration identification, and exchange of contact and other information before ENUM registrations begin. How to open a secure communication link and establish a session between a Tier 0/1 Registry and an SPR is not included in the provisioning procedures.
- An SPR can either provide its own Tier 2 Provider service or outsource the name server operation.
- An SPR may authorize its Tier 2 Provider to review/update certain data (e.g., host and technical contact information) at the Registry

### **8.2 Provisioning Requirements**

This section lists, or cross-references, the high level requirements for the entities involved in provisioning the ENUM.

#### **8.2.1 Tier 0/1 Registry**

The Tier 0/1 Registry is responsible for properly identifying and authenticating a SPR before accepting any transactions. The Tier 0/1 Registry is responsible for ensuring that SPRs comply with the requirements and procedures set out in the Registry agreement and monitoring SPR compliance.

#### **8.2.2 Service Provider of Record**

The Service Provider of Record must only register numbers for which they are identified in the LERG/NPAC as the network service provider.

The SPR must support the protocols specified between the Tier 1 Registry and the SPRs. The protocols include those for application handling, secure communications, and lower-layer transport/routing.

The SPR must follow the policies specified for Provider ENUM provisioning.

### **8.3 Provisioning Procedures**

This section describes representative scenarios for Provider ENUM Provisioning Activities. The Tier 0/1 Registry Operator shall develop a comprehensive set of procedures, subject to LLC approval. The

Registry Operator shall implement the procedures agreed upon and incorporate them into the Registry agreement.

### **8.3.1 Initial ENUM Registration**

#### **8.3.1.1 Assumptions**

#### **8.3.1.2 Provisioning Procedures**

1. The SPR establishes secure communication with the Tier 0/1 Registry and
2. The SPR provides registration information:
  - TN or TN range
  - A list of name server host names associated with the ENUM domain name(s)
  - SPR's information and technical and administrative contact information
3. The Registry authenticates the SPR and verifies the SPR's authority to register the TN based on the LERG and NPAC.
4. If the validation fails, the registration is rejected. If the validation is successful, the process continues with step 5.
5. Tier 0/1 Registry acknowledges to the SPR that the ENUM domain name registration is accepted. The Tier 1 Registry then performs the zone file updates to add the NS RRs of this ENUM domain name to its name servers. After the zone file updates have been performed at the Tier 1 Registry, real-time DNS queries for this particular ENUM domain name will be able to retrieve the name server information indicating where NAPTR RRs are hosted.

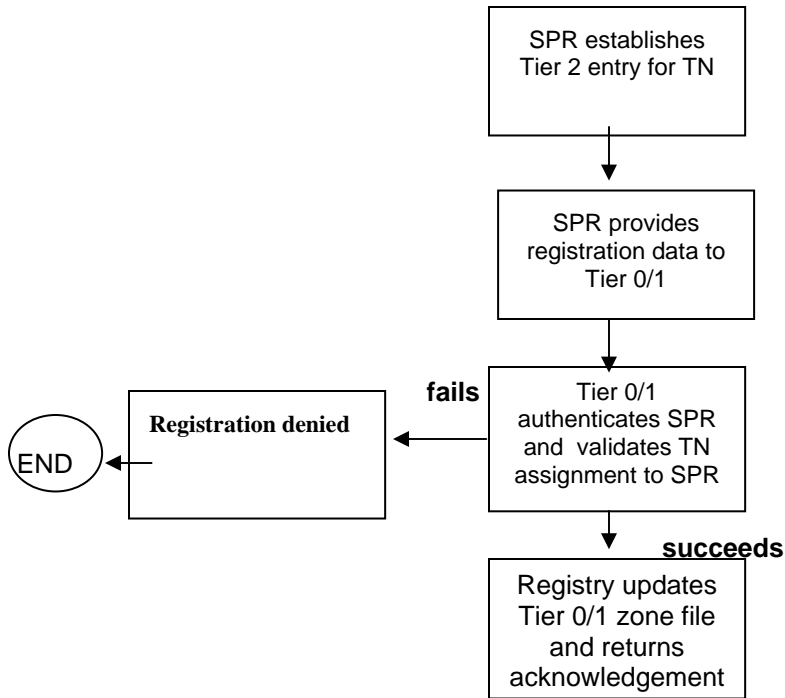


Figure 4. SPR register TN or TN range

### 8.3.4 *SPR Checks/Changes Information at Tier 0/1 Registry*

The SPR checks or changes information stored at the Tier 0/1 Registry.

#### 8.3.4.1 **Assumptions**

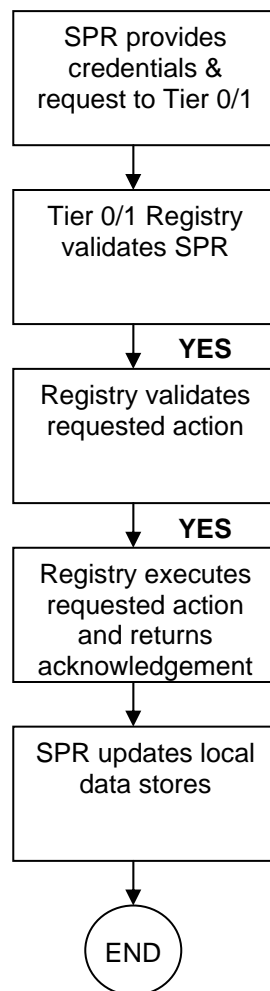
#### 8.3.4.2 **Provisioning Procedures**

1. The SPR provides the AAA-related information and indicates the type of request with the associated information to the Tier 0/1 Registry. The type of request and associated information may include:

- Check
  - All or certain current information associated with the ENUM Registrant's ENUM registration such as:
    - Contact information
    - service registration expiration date
    - The last date when an object is created, modified or transferred
    - State of an object (e.g., active, server hold)
  - All or certain current information associated with the SPRs data such as:
    - Contact information
    - Organizational information
    - IP address(es)
    - Security pass phrase (for authenticating an SPR when contacting the Tier 0/1 Registry's customer support by telephone)
    - User id and password information
  - Digital certificate information
- Add
  - Additional SPR Contact information
  - Additional SPR Organizational information
  - Additional IP address(es)
  - Additional user id and password
- Delete
  - Contact information
  - IP address(es)
  - SPR user id and password, when there are multiple accounts
- Modify/Change
  - SPR's contact information, user id, password, security pass phrase, digital certificate information, web site address

2. The Tier 0/1 Registry validates the SPR and, if the request is with respect to TN information, the SPR's authority over the TN based on the LERG and NPAC.

- a. If the validation fails, the Tier 0/1 Registry rejects the request indicating authentication/authorization failure (e.g., invalid password).
  - b. If the validation is successful, the Tier 0/1 Registry proceeds with Step 3.
3. The Tier 0/1 Registry checks whether the requested action is valid.
    - a. If the request is not valid (e.g., syntax error), the Tier 0/1 Registry rejects the request indicating the reason for rejection.
    - b. If the request is valid, the Tier 0/1 Registry performs the required actions and returns a positive acknowledgement.
  4. When a response is received, the SPR performs the following:
    - a. If the request is rejected, it tries to determine the cause of the failure and re-submit the request, if needed, after the problem is cleared.
    - b. If the request is accepted, it makes the necessary changes/additions/ deletions in the local data stores.



**FIGURE 5 – Flow Chart for 8.3.4.2:  
SPR Checks/Changes Information at Tier 0/1 Registry**

### 8.3.5 SPR Terminates ENUM Registration

The SPR terminates an ENUM registration.

#### 8.3.5.1 Assumptions

The ENUM registration is to be terminated.

#### 8.3.5.2 Provisioning Procedures

1. The SPR establishes secure communication with Tier 0/1 and requests removal of a TN registration providing the TN and necessary authentication information.
2. The Registry authenticates the SPR and the TN assignment.  
If YES, then proceed to step 3.  
If NO, the request is rejected and the reason indicated
3. The Tier 0/1 Registry removes the ENUM registration for that ENUM domain name from its local data store and name servers.
4. The Tier 0/1 acknowledges the successful execution of the request to the SPR.

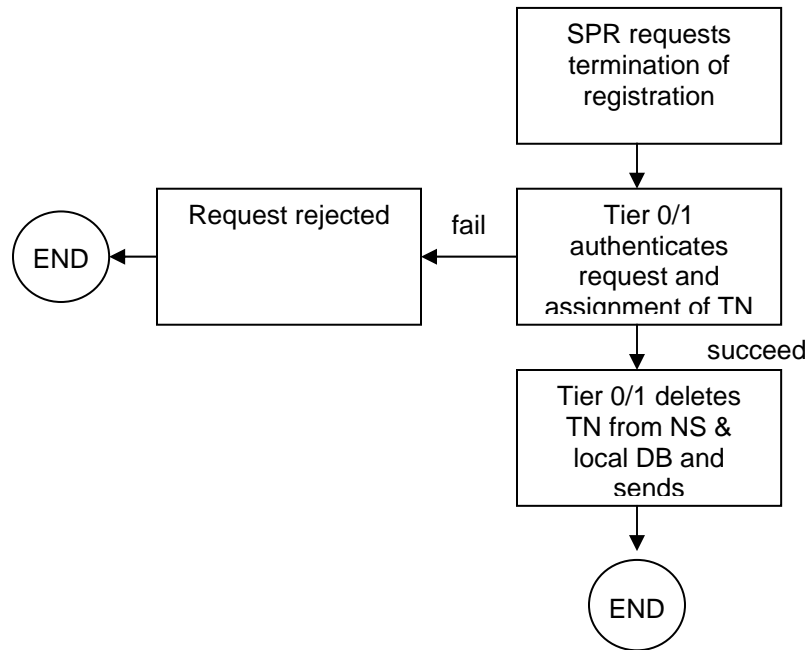


FIGURE 6 – Flow Chart for 8.3.6.2:  
SPR Terminates ENUM Registration

### 8.3.6 Number Port to new SPR

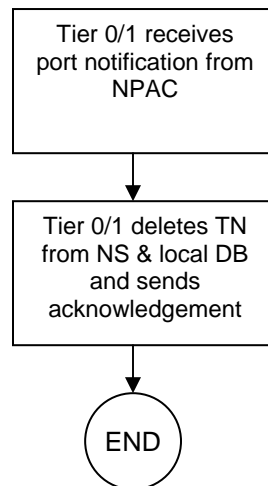
The number ports away from the current SPR.

### 8.3.6.1 Assumptions

- The Tier 0/1 determines that the number has ported to a new SPR
- In the absence of an automatic capability to create registration for the new SPR the registration is deleted.

### 8.3.6.2 Provisioning Procedures

1. The Tier 0/1 Registry determines from NPAC port notification that a number registered in Provider ENUM has ported.
2. The Tier 0/1 Registry deletes the existing ENUM registration for ported away number.
3. The Registry sends notification of the delete to the old SPR.



**FIGURE 8 – Flow Chart for 8.3.7.2:  
Number Ports Away from Current SPR**

## **8.4 Area Code Split**

An area code is split.

### **8.4.1 Assumptions**

- The Tier 0/1 Registry, the SPRs and the Tier 2 Providers that are involved with the telephone numbers (TNs) impacted by the area code split will take the necessary steps to support the area code split and the permissive dialing period<sup>5</sup>.
- The ENUM domain name that is associated with the TN under the old area code is referred to as the "old ENUM domain name." The ENUM domain name that is associated with the TN under the new area code is referred to as the "new ENUM domain name." For example, if the TN 703-434-1234 has registered for ENUM and is to be changed to 571-434-1234, the old ENUM domain name would be "4.3.2.1.4.3.4.3.0.7.1.e164enum.us," and the new ENUM domain name would be "4.3.2.1.4.3.4.1.7.5.1.e164enum.us." The TN under the old area code (e.g., 703-434-1234) is referred to as the "old TN," and the TN under the new area code (e.g., 571-434-1234) is referred to as the "new TN."
- Only the ENUM domain names that are associated with the TNs impacted by the area code split (those that are to be changed to the new area code) are discussed. ENUM domain names that are not impacted by the area code split are handled by the usual procedures. For example, if 703-538-6789 is not subject to the area code change, its associated ENUM domain name, 9.8.7.6.8.3.5.3.0.7.1.e164enum.us, will remain the same.
- T1 is the time (e.g., 12:01am EST on 6/1/01) when the new area code (e.g., 434 split from the old area code 804) becomes effective and the permissive dialing period begins. T2 is the time (e.g., 12:01am EST on 1/15/02) when the permissive dialing period ends.
- In area code relief activities there occur particular circumstances where individual 10 digit telephone numbers are changed. The Registry Operator must develop practices to ensure that the SPRs update the registry database with the correct information when this occurs.
- The Tier 0/1 Registry Operator shall monitor the North American Numbering Plan Administrator (NANPA) website (<http://www.nanpa.com>) for impending area code splits (see NPA Relief Planning Letter), and use other information sources (e.g., the "area code split exchange diskette" from Telcordia (<http://www.trainfo.com>)) as needed to maintain an up-to-date list of the affected NPA-NXX codes for a particular area code.

### **8.4.2 Provisioning Procedures**

#### **8.4.2.1 Procedures/Guidelines for a Tier 0/1 Registry with a Permissive Dialing Period**

At no time before the T1 shall the Tier 0/1 Registry accept any request on any new ENUM domain name from the SPR. This is because the new TN under the new area code is not yet effective before T1.

---

<sup>5</sup> The permissive dialing period is the interval during which the TN under either the old area code or the new area code can be dialed to reach the same termination. The length of the permissive dialing period is normally a few months and is set by the state Public Utility Commission for each involved area code.

Starting at T1, the Tier 0/1 Registry shall be capable of accepting and responding to any request made on the new ENUM domain name from the SPR, and shall perform data updates on the local data stores and zone files, if applicable.

The Tier 0/1 Registry shall not accept any request on any old ENUM domain name from the SPR during the permissive dialing period.

At T1, the Tier 0/1 Registry shall perform zone file updates to add all the new ENUM domain names. One, or more than one, new zone files may be created, or new data is added, to the existing zone file for those new ENUM domain names with exactly the same name server information copied from those associated with the corresponding old ENUM domain names at T1.<sup>6</sup> The Tier 0/1 Registry shall not remove the Name server (NS) Resource Records (RRs) associated with the old ENUM domain names from the existing zone file(s).

The Tier 0/1 Registry Operator should progressively reduce the Time to Live (TTL) values for the resource records associated with the old ENUM domain name so that such records will not persist in resolver caches beyond T2.

The TTL in the NS RRs associated with the new ENUM domain name is set to a typical value (e.g., from a day to a week) depending on the Tier 0/1 Registry policy (e.g., frequency of zone file updates).

Within twenty-four hours after T1, the Tier 0/1 Registry shall update its stored information to reflect the area code change on all the TNs. It shall search the local data stores and change all the TNs that are subject to the area code change, not just those that are associated with the old ENUM domain names. This will change all the phone numbers and fax numbers in the contact information of all the records.

The Tier 0/1 Registry shall not accept any request (e.g., create, check, update, renew or transfer) on any old ENUM domain name during the permissive dialing period while it maintains records associated with the old ENUM domain name.

The Tier 0/1 Registry shall keep the name server information in the zone file, and information in the local data stores associated with each new ENUM domain name, synchronized with those associated with the corresponding old ENUM domain name during the permissive dialing period. Any update request on the new ENUM domain name that is received from the SPR during the permissive dialing period shall cause the same update on the old ENUM domain name. This includes the data in the ContactInfo database in case there are inquires about the ContactInfo information on the old ENUM domain names.

During the permissive dialing period, if the Tier 0/1 Registry receives a create request for an ENUM domain name that is available (e.g., no record exists for this ENUM domain name) and the associated TN is a new TN due to an area code split, it shall create a record for the old ENUM domain name in addition to the record for the new ENUM domain name.

At T2, the Tier 0/1 Registry shall perform zone file updates to remove the NS RRs associated with the old ENUM domain names. It shall remove all the records associated with the old ENUM domain names from the local data stores.

After the permissive dialing period expires, the Tier 0/1 Registry shall expect new ENUM registrations on the old ENUM domain names in accordance with the requirements for the area code split. Within twenty-four hours after T2, the Tier 0/1 Registry should send an e-mail message to each technical contact that is associated with each old ENUM domain name to remind them to update the zone file(s) by removing any

---

<sup>6</sup> The new and old ENUM domain names may or may not be in the same zone file depending on how the zones are cut/delegated.

RR in the zone file and the data in the local data stores that is associated with the old ENUM domain name.

#### **8.4.2.2 Procedures/Guidelines for a Tier 0/1 Registry without a Permissive Dialing Period**

Since there is no permissive dialing period, T1 and T2 are the same. T1 in this case is the time when the new TN must be dialed and the old TN must not be dialed.

One week before T1, it is recommended that the Tier 0/1 Registry Operator send an e-mail message to each associated SPR about the area code split and to remind them to take the appropriate actions required by the area code split.

At no time before T1 shall the Tier 0/1 Registry accept any request on any new ENUM domain name from the SPR. This is because the new TN under the new area code is not yet effective before T1.

The Tier 0/1 Registry should progressively reduce the Time to Live (TTL) values for the resource records associated with the old ENUM domain name so that such records will not persist in resolver caches beyond T1.

At T1, the Tier 0/1 Registry shall perform zone file updates to change all the old ENUM domain names to the new ENUM domain names while keeping the name server information unchanged. This can also be done by adding the NS RRs for the new ENUM domain names and removing those associated with the old ENUM domain names when dynamic updates are done. The TTL in the NS RRs associated with the new ENUM domain names should be set to a typical value (e.g., from a day to a week) depending on the Tier 1 Registry policy (e.g., frequency of zone file updates).

Starting at T1, the Tier 0/1 Registry shall be capable of accepting and responding to any request made on the new ENUM domain name from the SPR and shall perform data updates on the local data stores and zone files, if applicable.

Within twenty-four (24) hours after T1, the Tier 0/1 Registry shall update its stored information to reflect the area code change on all the TNs. It shall search the local data stores and change all the TNs that are subject to the area code change, not just those that are associated with the old ENUM domain names. This will change all the phone numbers and fax numbers in the contact information of all the records.

After T1, the Tier 0/1 Registry shall expect new ENUM registrations on the TNs under the old area code because the associated TNs can be reassigned to new telephony subscribers.

#### **8.4.2.3 Procedures/Guidelines for an SPR with a Permissive Dialing Period**

The SPR should be aware of any area code split and the associated T1 and T2 that impacts the ENUM domain names registered through it. The Tier 0/1 Registry Operator will notify SPRs of impending area code splits.

One week before the SPR shall update the zone file(s) by adding the NS RRs and the Naming Authority Pointer (NAPTR) RRs for the new ENUM domain name before T1 and to leave the NS RRs and the NAPTR RRs associated with the old ENUM domain names in the existing zone file(s) until the permissive dialing period expires.

Within twenty-four hours after T1, the SPR should update its stored information to reflect the area code change on all the TNs. It shall search the databases and change any TN that is subject to the area code change. This will change all the phone numbers and fax numbers in the contact information in all the records.

During the permissive dialing period, if the SPR should submit a create request only on the new ENUM domain name and shall have the NAPTR RRs that are associated with both the new and old ENUM domain names in the Tier 2 name servers.

The ENUM Registrant may inform the SPR about the TN change whether it is related to the ENUM domain name or any phone or fax number. The SPR can confirm/ignore the update request if the change has been made automatically and may double check whether the change has been made correctly.

Within twenty-four hours after T2, the SPR update the Tier 2 zone file(s) by removing any RR in the zone file and the data in the local data stores that are associated with the old ENUM domain name.

#### **8.4.2.4 Procedures/Guidelines for an SPR without a Permissive Dialing Period**

The SPR should be aware of any area code split and the associated T1 that impacts the ENUM domain names registered through it. The Tier 0/1 Registry Operator will notify SPRs of impending area code splits.

One week before T1, the SPR shall update the Tier 2 zone file(s) by adding the NS RRs and the NAPTR RRs for the new ENUM domain name, and by removing those RRs associated with the old ENUM domain name at T1.

Within five minutes after T1, the SPR shall update its stored information to reflect the area code change on all the TNs. It shall search the databases and change any TN that is subject to the area code change. This will change all the phone numbers and fax numbers in the contact information in all the records.

▪ **SECTION 9.0           DISPUTE RESOLUTION**

---

Because determination of Service Provider of Record is based on the LERG and NPAC a dispute resolution process like that planned for User ENUM is not required for Provider ENUM. Disputes concerning registrations rights to a TN must be resolved through PSTN processes leading to LERG/NPAC updates which will then be faithfully reflected by the Tier 0/1 Registry.

▪ **SECTION 10.0        TIER 0/1 REGISTRY REPORTING**

---

The Registry Operator should make available regular reports for the SPRs on the daily, weekly, and monthly activity. The monthly level report should provide the necessary details for end of month billing. Further more a monthly report on performance and major activities should be reported to the contracting authority and all designated government agencies.

**10.1   Tier 0/1 Registry Reporting for SPRs**

The Registry Operator should provide daily, weekly, and monthly reports that are available to SPRs via a secured file transfer protocol (FTP) server. To assist SPRs in their ability to monitor their registration activity throughout the month, the Tier 0/1 registry should generate separate daily and weekly reports for each of its SPRs, as listed in Table 3 below.

SPRs are able to use these reports to monitor their registration activities and to reconcile their activity to the monthly billing reports. These reports are published on the first day of each month and provide SPRs with a means to reconcile their monthly invoices to their transaction activities, listed below:

- \* Registrations
- \* Syncs
- \* Deletions
- \*Port outs
- \*Port ins

The reports reflect the actual activity for the period that affected the SPR account. The SPRs receive one monthly invoice reflecting the counts for all billable activity for the month and the details behind the summary counts on the invoice are provided in the detail reports identified above. The system associates a transaction ID with every transaction that occurs in the system. These transaction IDs provide an audit trail of all financial transactions allowing SPRs, as well as the Tier 0/1 personnel, to easily trace activity during the audit process.

**Table 3 SPR Reports provided by Tier 0/1**

<b>Report Name</b>	<b>Report Features</b>
Daily Transactional SPR Report	Lists all SPR-Registry transactions that occurred on previous day
Daily SYNC Report	Lists all domains that were synced previous day
Daily Delete Report	Lists all domain names deleted
Weekly Domain Name Report	Cumulative report of all domain names managed by SPR; Lists domain name, create date,
Weekly Domains Hosted by Name Server Report	Lists all domains hosted by your name servers; Lists name server and domain names.
Monthly Billing Detailed Report	Developed for each SPR to capture detailed billable transaction events

**10.2 Tier 0/1 Registry Operator Reporting to LLC**

On a monthly basis the Tier 0/1 should provide a report to the LLC that provides performance details and major activities. In Table 4 is a list of recommended data to be reported.

**Table 4 Monthly LLC report provided by Tier 0/1**

SPR Status.
Service Level Agreement Performance
TLD Zone File Access Activity
Completed EPP interface software releases
Domain Names Under Sponsorship – Per SPR
Name Servers Registered – Per SPR
Domain Names Registered by Registry Operator
Contact Info Service Activity
Total Monthly Contact Info Queries
Total Monthly Domain Name Transaction Trend by Category
Total Monthly Name Server Transactions by Category

(Additions, Modifications, Deletions) by SPR by NPA
Average Daily Transaction Range
E.164 Geographical Registrations Distribution
Deleted Names - Per SPR
Other Information <ul style="list-style-type: none"> <li>a) Total Monthly Transactions by Category</li> <li>b) Total Transactions by Month</li> <li>c) Registrations Distribution for reporting month</li> </ul>

**10.3**

▪ **SECTION 11.0      PRIVACY CONSIDERATIONS**

---

Provider ENUM data are intended primarily for use by service providers for the purpose of effecting interconnection. While this is simplified by having at least an initial AoR available in the public DNS, care in implementation is required to protect customer privacy. In particular, the following should be observed by SPRs in registering numbers into Provider ENUM.

- AoRs should not include information that would associate a person with a telephone number
- AoRs should identify carrier network elements rather than user customer premises equipment
- To prevent data miners from identifying active non-published numbers by identifying numbers registered in Provider ENUM that are not present in directory listings, SPRs should register all allocated TNs in blocks that contain TNs that they wish to register, whether or not those TNs are currently assigned and whether or not the SPR supports interconnection via ENUM for those TNs (in the latter case a tel URI can be provided in the registration.)