

June 30, 2005
CC1 ENUM LLC
Technical Advisory Committee

Technical and Operational Requirements for an ENUM Tier 1A Registry for Country Code 1

CC1 ENUM LLC

Abstract

This document contains technical and operational requirements for operating an ENUM Tier 1A for Country Code 1. This includes interfaces to other entities providing services for ENUM as well as the requirements for deploying and operating the ENUM Tier 1 infrastructure.

FOREWORD

At the time it approved this document, the CC1 ENUM LLC TAC had the following members:

Jim Baskin	TAC Chairman, Verizon
Jay Carpenter	1-800 AFTA
Andrew Gallant	AG Design, LLC
Steven D. Lind	AT&T
Penn Pfautz	AT&T
Doug Birdwise	Bell Canada
Ken Buchanan	BellSouth
Mark McFadden	BT Americas
Tim Denton	CIRA
Chip Sharp	Cisco
Tom Creighton	Comcast
Jason Livingood	Comcast
Suzanne Howard	COX
Beth O'Donnell	COX
Tim Ruiz	GoDaddy.com
Judith Oppenheimer	ICB
Blaine Elzey	Lucent
Doug Rollender	Lucent
Ron Santos	Lucent
Karen Mulberry	MCI
Robert Schafer	MCI
Alan Johnston	MCI
Richard Shockey	NeuStar
Mike St. Johns	Nominum
Bernie Ku	SBC Labs
Phyllis Anderson	SBC Labs
Jim Danda	Sprint
Mir Islam	Sprint
Hala Mowafy	Telcordia
Kaj Tiesink	Telcordia
Kevin McCandless	Verisign

TABLE OF CONTENTS

Foreword.....	ii
Table of Contents.....	ii
Table of Figures.....	iii
1. Scope, Purpose, and Application	1
1.1 Scope.....	1
1.2 Purpose	1
1.3 Application.....	1
2. References.....	1
3. Definitions, Acronyms, & Abbreviations.....	3

CC1 ENUM LLC TAC — June 30, 2005 version - final

3.1 Definitions3

3.2 Acronyms & Abbreviations.....3

4. Introduction.....4

5. Operational & Infrastructure Requirements.....6

5.1 Tier 1A Registry Operation6

5.1.1 Registry Database6

5.1.2 Zone Data.....7

5.1.3 Contact Info7

5.1.4 Reports and Files7

5.1.5 Database Escrow and Backup7

5.1.6 Network Operations and Maintenance8

5.1.7 System Outage Prevention8

5.1.8 System Recovery Procedures8

5.1.9 Technical and Other Support.....9

5.2 Domain Name System Requirements.....9

5.3 Security.....9

5.3.1 Operational System Security9

5.3.2 Physical Security9

5.3.3 Network Security10

5.3.4 Backup Security11

5.3.5 Security Audit and Reporting.....11

5.4 Other Responsibilities of the Tier 1A Registry11

5.5 Transition Requirements12

6. Service Level Requirements12

6.1 Service Availability12

6.2 Processing Time13

6.3 Update Latency13

6.4 Cross-Network Name Server Performance (CNNP) Requirements13

TABLE OF FIGURES

FIGURE 1 - ENUM FUNCTIONAL ARCHITECTURE5

Technical and Operational Requirements for an ENUM Tier 1A Registry for Country Code 1

1. SCOPE, PURPOSE, AND APPLICATION

1.1 *Scope*

This document describes the technical and operational requirements for an ENUM Tier 1A Registry for Country Code 1 (CC1) under the ITU-T E.164 international numbering standard.

Tier 1A is a single Internet domain name system (DNS) zone intended to be common to all nations that share country code 1 of the ITU-T E.164 international numbering standard.

The registry for the Tier 1A zone will be used as the registry (the *root*) for all North American Numbering Plan (NANP) Numbering Plan Areas (NPA), such as 202, 613, 800, 866, 900, etc.

Tier 1A will be used to register both geographic NPAs, that is NPAs better known as Area Codes, but shall also be capable of supporting non-geographic resources such as toll free and caller-pays 900 services.

1.2 *Purpose*

This document is intended to provide the specifications necessary to implement the components for ENUM for geographic Numbering Plan Area resources within the Country Code 1. It should provide sufficient information to allow a contracting entity to put out a request for proposal to business organizations in the industry. As such, it describes, among other things, the reference architecture for the Tier 1A portion of ENUM, the operational and administrative aspects of the Tier 1A Registry, and the provisioning process. It also addresses the critical security and privacy issues inherent in implementing this system.

The immediate audience of this document is comprised of CC1 ENUM LLC, ENUM Forum members, Canadian Steering Committee on Numbering members, NTIA, FCC, Industry Canada, Canadian Radio-television and Telecommunications Commission (CRTC), CIRA, national numbering administrations for NANP member countries and all other stakeholders such as potential users of ENUM. This document is being distributed to all stakeholders with a view to seeking consensus amongst an audience that is as large as possible, with a view of ensuring that the implementation of ENUM CC1 Tier 1A proceeds as swiftly and as smoothly as possible.

1.3 *Application*

This document is intended to serve as a basis for establishing consensus for preparing a memorandum of understanding between the industry and government entities in Country Code 1, with a view to preparing the request for proposals for the management of Country Code 1 in ENUM and the ultimate selection of the vendor that shall provide Country Code 1 Tier 1A services.

2. REFERENCES

The following references contain provisions that are incorporated by reference to this specification. At the time of publication, the editions indicated were valid. All documents are subject to revision, and

CC1 ENUM LLC TAC — June 30, 2005 version - final

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] [Falstrom, P., Mealling, M., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.
- [2] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.
- [3] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.
- [4] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.
- [5] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
- [6] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
- [7] Mockapetris, P., "DNS encoding of network names and other types", RFC 1101, April 1989.
- [8] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.
- [9] Elz, R., Bush, R., Bradner, S. and M. Patton, "Selection and Operation of Secondary DNS Servers", BCP 16, RFC 2182, July 1997.
- [10] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
- [11] Eidnes, H., de Groot, G. and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.
- [12] M. Horowitz & S. Lunt, "FTP Security Extensions" RFC 2228, October 1997.
- [13] M. Allman & S. Ostermann, "FTP Security Considerations," RFC 2577, May 1999.
- [14] M. Ohta, "Incremental Zone Transfer in DNS," RFC 1995, August 1996.
- [15] P. Vixie, "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)," RFC 1996, August 1996.
- [16] P. Vixie, S. Thomson, Y. Rekhter, & J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," RFC 2136, April 1997.
- [17] P. Vixie, "Extension Mechanisms for DNS (EDNS0)," RFC 2671, August 1999.
- [18] M. Crawford & C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering," RFC 2874, July 2000.
- [19] D. Eastlake 3rd, "DNS Request and Transaction Signatures (SIG(0)s), " RFC2931, September 2000.
- [20] R. Bush, D. Karrenberg, M. Kosters, & R. Plzak, "Root Name Server Operational Requirements," RFC2870, June 2000.
- [21] Arends, R. et al, "DNS Security Introduction and Requirements," RFC2870", RFC4033, March 2005
- [22] Arends, R. et al, "Resource Records for the DNS Security Extensions", RFC4034, March 2005
- [23] Arends, R. et al, "Protocol Modifications for the DNS Security Extensions", RFC4035, March 2005
- [24] Vixie, P., "Extension Mechanism for DNS (EDNS0)", RFC2671, June 1999
- [25] Crawford, M., "Non-Terminal DNS Name Redirection", RFC2672, August 1999
- [26] Thomson, S. et al, "DNS Extensions to Support IP Version 6", RFC3596, October 2003
- [27] Eastlake, D. 3rd, "DNS Request and Transaction Signatures (SIG(0)s)", RFC2931, September 2000.

3. DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions

ENUM

ENUM is a protocol developed in the Internet Engineering Task Force (IETF) (initially in RFC 2916 superseded by RFC 3761) whereby the “Domain Name System (DNS) can be used for identifying available services connected to one E.164 number.”

3.2 Acronyms & Abbreviations

CC1	Country Code 1
CIRA	Canadian Internet Registration Authority
CNNP	Cross Network Name Server Performance
CRTC	Canadian Radio-television and Telecommunications Commission
DNS	Domain Name System
DNSSEC	DNS Security Extensions
FCC	Federal Communications Commission
FTP	File Transfer Protocol
HVAC	Heating, Ventilating, and Air Conditioning
IETF	Internet Engineering Task Force
ITU-T TSB	International Telecommunication Union – Telecommunication Standardization Sector, Telecommunication Standardization Bureau
NANP	North American Numbering Plan
NANPA	North American Numbering Plan Administrator
NPA	Numbering Plan Area
NAPTR	Naming Authority Pointer
NS	Name Server
NTIA	National Telecommunications and Information Administration
PoP	Point of Presence
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
SCP	Secure Copy
SRS	Shared Registration System
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Universal Resource Identifier
WWW	World Wide Web

4. INTRODUCTION

This section specifies the reference architecture of a single common ENUM DNS domain, 1.e164.arpa, within Country Code 1.

ENUM implementation is based on a tiered architecture as shown in Figure 1. At Tier 0 is the RIPE NCC, which maintains the e164.arpa zone.¹ Entries in the RIPE NCC name servers correspond to country codes and point to the name servers of the Tier 1 Registry that is authoritative 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 nations, the plan of the CC 1 ENUM 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 states. 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. The detailed technical requirements for the Tier 1B are contained in a separate document developed by the CC1 ENUM LLC Technical Advisory Committee.

CC1 ENUM Tier 1B registry(ies) will be required to establish a business relationship with the CC1 ENUM Tier 1A Registry prior to registering any NPA in e164.arpa. The nature of the business relationship will be defined by the contracting entity, 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 Tier 1B 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.

ENUM Registrars, the entities that accept registration requests from number assignees, will, in turn, be required to establish a business relationship with the CC1 ENUM Tier 1B registry(ies) prior to registering any telephone number, in e164.arpa. The nature of the business relationship between the Tier 1B and the ENUM registrars will be defined by the contracting entity, embodied in a Registry agreement, and will be the same for all ENUM Registrars for a given NPA entered into Tier 1A. This is necessary to ensure competitive equity between registrars in Tier 1B and to ensure that ENUM Registrant's records are properly maintained and that the assignee of the E.164 telephone number has decided to participate in ENUM.

¹ The instructions regarding operations of the domain e164.arpa can be found at the URL: <http://www.ripe.net/rs/enum/instructions.html>

The ITU-T TSB evaluates 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/>

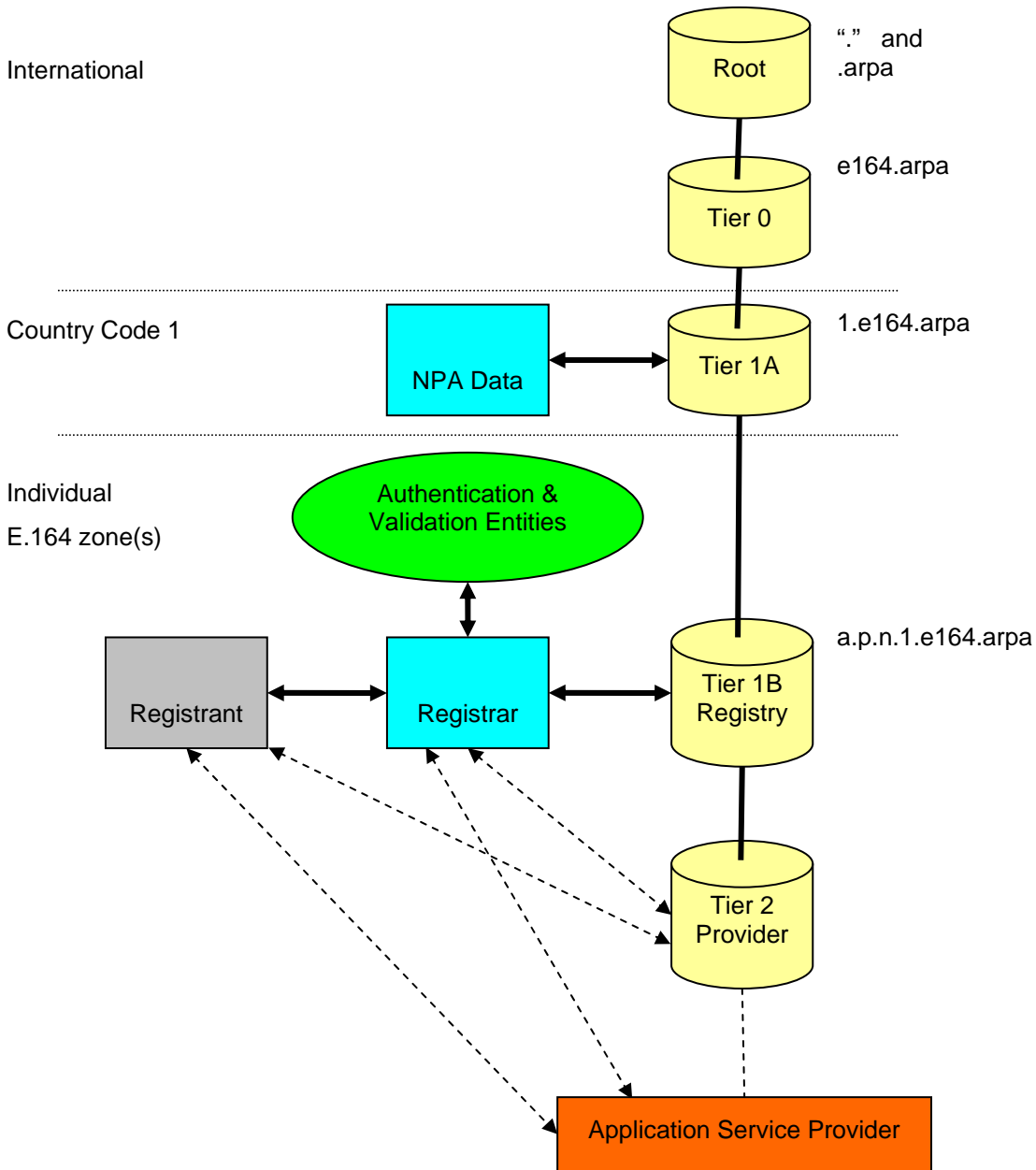


Figure 1 - ENUM Functional Architecture

The Tier 2 Provider for an E.164 number maintains the actual NAPTR records that contain URIs (Universal Resource Identifiers) for specific communication services, and the Application Service Provider uses these records to provide those services to the number assignee (the Registrant.)

5. OPERATIONAL & INFRASTRUCTURE REQUIREMENTS

This section provides requirements for the operation and infrastructure of the ENUM Tier 1A registry. Service Level Requirements are contained in Section 6.

5.1 Tier 1A Registry Operation

This section specifies the technical requirements for the operations of a Country Code 1 Tier 1A Registry.

A Tier 1A Registry will maintain the addresses of the name servers of the Tier 1B registries in Country Code 1 that national authorities for the respective Tier 1B registries have authorized. The Tier 1A Registry shall:

- Check with NANP Administration to identify the nation to which the NPA has been allocated and verify that the party making the request is authorized to act in that capacity by its national authority.
- Provide procedures that will allow the Tier 1B operators to manage the records for their NPAs in the Tier 1A registry.

The Registry shall also have the capability to maintain the addresses of the Tier 1B name servers for the non-geographic NPAs, such as 800, 888, etc. and allow the corresponding Tier 1B operator(s) to manage records for such NPAs. Based on guidance from NANP member nations, the CC1 ENUM LLC will inform the Registry as to the Tier 1B for a given non-geographic NPA.

5.1.1 Registry Database

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

A Tier 1A Registry should describe how it would meet the following requirements for an ENUM Registry database.

A Registry database:

- Shall be sized to accommodate the expected demand at initial launch, and to support growth without interruption as ENUM matures.
- Shall be able to perform transactions at a rate that meets the needs of the Tier 1B Registries.
- 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. Tier 1A candidate 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. Because the Tier 1A registry will likely contain fewer than a thousand records and additions and changes are expected to be infrequent, a mechanized interface or system (Shared Registration System) between Tier 1Bs and the Tier 1A should not be required. However, transport of records between the Tier 1Bs and Tier 1As shall be via a secure methodology. If and when the CC1 ENUM LLC elects to require

implementation of DNSSEC, the Tier 1A Registry must revise the interface accordingly and, thus, may want to plan for this circumstance in the initial design.

5.1.2 Zone Data

Zone data consists of the technical information that the DNS requires to function correctly. Zone data generation, or zone data propagation, is the term traditionally used to describe the process of generating zone information from the Registry database and deploying the data to the DNS database

The Tier 1A registry shall meet the following requirements for zone operations:

- Provide a means to generate the zone data from the Registry database to the DNS database to timely reflect any changes as defined in the Service Level Requirements.
- Reliably and securely propagate the zone data to all Tier1A name servers with minimum delay.
- The frequency of zone data generation and the delay of zone file propagation shall meet the needs of the ENUM users.
- Zone data generation and propagation procedures shall be carefully engineered so that they will not adversely affect the normal Registry and name server operations.
- Zone data distribution procedures shall conform to appropriate IETF standards.
- There shall be at least four geographically dispersed (separated by at least 200 miles) name servers for an ENUM Tier 1A Registry.
- At least two of the Tier 1A name servers must be located within the United States.

5.1.3 Contact Info

The Tier 1A Registry shall make publicly available contact information (Contact name or title, email address, phone, fax, organization and organizational entity, etc.) for the Tier 1B Registries associated with each NPA, for instance, on a web page.

5.1.4 Reports and Files

An ENUM Tier 1A Registry shall provide reporting service to allow ENUM Tier 1B Registries to retrieve reports on performance statistics for resolving the entries in Tier 1A. In addition, it may also make available complete NPA zone file to appropriate entities as defined by the CC1 ENUM LLC.

A Tier 1A Registry shall provide appropriate reporting capabilities for national authorities, Tier 1B Registries and the CC1 ENUM LLC, including, at a minimum, registry performance and zone data transactions. It shall maintain transaction logs for this purpose.

5.1.5 Database Escrow and Backup

The goal of any data backup/recovery procedure is full 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.

A Tier 1A candidate 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
- How escrow and back-up data will be used for recovery

In addition, the following safeguards are required of the Tier 1A registry:

- 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

5.1.6 Network Operations and Maintenance

ENUM is envisioned as a completely robust and high-availability service. The Tier 1A shall operate and maintain the various aspects of the Registry to a high service level. Bidders should include descriptions of how they intend to ensure system outage prevention, system recovery procedures, and technical support, including arrangements for power, HVAC (Heating, Ventilating, and Air Conditioning), and fire systems.

5.1.7 System Outage Prevention

The Tier 1A Registry requires outage prevention measures specifically designed to minimize system component downtime. Downtime can be either unplanned, which is caused by failures in external telecommunications, power, or internal network or computer equipment; or planned, which occurs when the system is unavailable due to scheduled maintenance (e.g., during software or hardware upgrades and system backups).

A Registry shall:

- Use redundancy and high-availability system architectures to eliminate planned downtime of the whole system. That is, the Registry service shall remain operational when part of the system is undergoing software or hardware upgrades and system backups.
- Use redundancy and high-availability system architectures to minimize individual server unplanned downtime.
- Employ a comprehensive set of system monitoring procedures for problem detection and resolution at multiple levels of the architecture, including processor, memory, operating system, database, application process, and network connectivity.
- Make available backup software, operating systems, and hardware in all data centers.
- Employ a streamlined technical support process to ensure that the appropriate staffs resolve all problems in a timely manner
- Incorporate appropriate geographic and network diversity in its architecture
- Track and report any outage planned or unplanned which prevents any server from answering a query.

5.1.8 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.

The Tier 1A registry shall meet the following operations and maintenance requirements:

- 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
- Active and Passive attacks

In addition, a Registry should:

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

5.1.9 Technical and Other Support

The Tier 1A Registry must act as technical liaison with Tier 0 for resolution of issues with respect to the delegation of authority over 1.e164.arpa in CC1.

The Tier 1A Registry must provide technical and other support to the Tier 1B Registries from an appropriate customer help desk with a well-defined escalation policy.

5.2 Domain Name System Requirements

The Tier 1A Registry must comply with relevant IETF RFCs and best practices including specifically RFC 2870. The bidder must identify other relevant RFCs with which it complies.

5.3 Security

A Tier 1A must secure both Registry operations and data. A Registry 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 shall define and implement multi-tiered procedures that provide security protections to all parts of the Registry system

5.3.1 Operational System Security

- Protection/Prevention of compromise of the systems hosting or managing Tier 1A
- 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 1A and 1B service (name servers, registry, etc)
- Encryption requirements
- Authentication & Authorization requirements
- Requirements on ISPs providing connectivity for Tier 1A

5.3.2 Physical Security

- The Tier 1A Registry 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.
- 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.

5.3.3 Network Security

- User identification, passwords, and IP range checking shall be required 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 1Bs and the Tier 1A Registry [RFC 2228, RFC 2577, or similar equivalent].
- 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.
- Checks shall take place on all 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 1A 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 1A Registry 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.

5.3.4 Backup Security

- Backup shall be performed through a secure network on the main Tier 1A Registry site.
- The Tier 1A Registry 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.

5.3.5 Security Audit and Reporting

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

- The Tier 1A Registry 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 1A Registry data. Bidders should detail the hierarchy of breach severity and escalation procedures.
- The Tier 1A Registry shall provide a monthly security status report to the CC1 ENUM LLC, including a list of security incidents categorized by severity.

5.4 Other Responsibilities of the Tier 1A Registry

The Tier 1A Registry will use commercially reasonable efforts to restore the critical components of an affected Tier 1A Registry site within 48 hours in the case of a *force majeure* event. No single event shall result in an outage of DNS resolution service itself.

The Tier 1A Registry will perform internal monitoring as a means to verify that the availability and performance measurements of this document are being met. In the case of name server performance requirements, a mutually agreed upon third party verification entity will be used.

Beginning no later than 120 days after the commencement-of-service date, the Tier 1A Registry will provide monthly system performance and availability reports to the contracting entity, subject to the determination of the contents of the report by the contracting entity.

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

5.5 *Transition Requirements*

The Tier 1A Registry must provide a plan for transitioning of the Registry to a new provider within the timeframe set forth in the terms and conditions in the Registry contract. The plan must ensure no disruption of ENUM DNS service.

6. SERVICE LEVEL REQUIREMENTS

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

- 100 percent availability for resolution services
- 100 percent accuracy of the zone file

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

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 Tier 1B 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 Tier 1B 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 Tier 1B. 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.

6.2 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 Services. Processing Time Performance Specifications will be measured in a Monthly Timeframe and will be reported on a monthly basis to the CC1 ENUM LLC.

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.

6.3 Update Latency

The Registry Operator makes timely updates to the data on the DNS Name Servers in response to requests from the Tier 1B Registries. The Tier 1A Registry Operator processes these updates on a near real time basis. This is measured from the time that the registry verifies the update request to the time the update appears in the DNS Name Server. Update latency performance will be reported on a monthly basis.

During normal business hours, the Tier 1A Registry shall implement authorized changes (e.g., change to or addition of an NS record for an existing assigned NPA) requested by Tier 1B registries within 15 minutes. The Registry shall also provide procedures for emergency out-of-hours changes.

6.4 Cross-Network Name Server Performance (CNNP) Requirements

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 under 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 1A's DNS Name Servers and observing the responses from the Tier 1A'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.

CC1 ENUM LLC TAC — June 30, 2005 version - final

- 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 1A 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 1A name server must not exceed the required values.
 - b) The packet loss to each of the Tier 1A 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.