

Network Working Group
Request for Comments: 4725
Category: Informational

A. Mayrhofer
enum.at
B. Hoeneisen
Switch
November 2006

ENUM Validation Architecture

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The IETF Trust (2006).

Abstract

An ENUM domain name is tightly coupled with the underlying E.164 number. The process of verifying whether or not the Registrant of an ENUM domain name is identical to the Assignee of the corresponding E.164 number is commonly called "validation". This document describes validation requirements and a high-level architecture for an ENUM validation infrastructure.

Table of Contents

1. Introduction	3
2. Requirements	3
3. ENUM Provisioning Model and Roles	4
3.1. Number Assignment Entity (NAE)	5
3.2. Assignee	7
3.3. Registrant	7
3.4. Validation Entity (VE)	7
3.5. Registry	8
3.6. Registrar	8
3.7. Domain Name System Service Provider (DNS-SP)	8
3.8. Application Service Provider (ASP)	8
4. Validation Process Assumptions	9
4.1. Workflow	9
4.2. Trust Relations	10
4.3. Data Flow and Format	11
5. Example Scenarios	11
5.1. E.164 Number Assignment along with ENUM Registration	11
5.2. Fully Disjoint Roles	13
6. Security Considerations	14
6.1. Fraud Prevention	14
6.2. Assignee Data	14
7. Acknowledgements	15
8. References	15
8.1. Normative References	15
8.2. Informative References	15

1. Introduction

E.164 Number Mapping (ENUM) [1] uses the Domain Name System (DNS) [4] to refer from E.164 numbers [2] to Uniform Resource Identifiers (URIs) [3]. E.164 numbers are mapped to domain names through means described further in RFC 3761 [1].

"Ordinary" domain names are usually allocated on a first-come-first-served basis, where the associated registration data is the complete source of ownership. However, ENUM domain names are linked to E.164 numbers, and thus intrinsically tied to the status and the "Assignee" (defined in Section 3.2) of the corresponding E.164 number.

2. Requirements

Preserving integrity between ENUM and E.164 is one of the main concerns in ENUM implementations, and often one of the reasons why "trials" precede commercial implementations.

To maintain this relationship between E.164 numbers and ENUM domain names, registration processes must ensure that the following requirements are fulfilled during the entire lifetime of an ENUM delegation:

- o The ENUM domain name corresponds either to an assigned E.164 number or to a respective E.164 number that is assigned during the registration process itself.
- o The corresponding E.164 number is within a number range approved to be used with ENUM.
- o The registration of the ENUM domain name is authorized by the Assignee of the corresponding E.164 number; i.e., the entity requesting the registration of an ENUM domain name is either the Assignee of the corresponding E.164 number itself or an entity authorized to request registration on behalf of said Assignee.
- o The "Registrant" (see Section 3.3) of the ENUM domain is identical to the Assignee of the corresponding E.164 number.

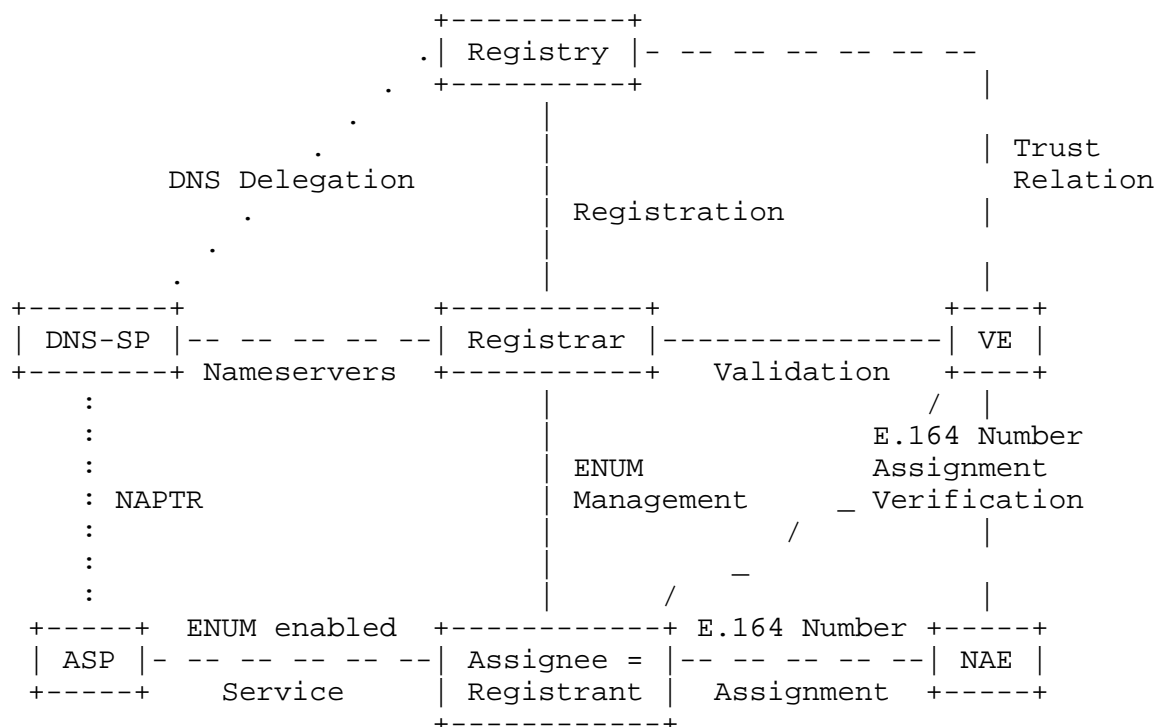
The process of verifying the above requirements during registration is commonly called "initial validation". In addition to this one-time validation process, provisions must be made that ENUM domain name delegations are revoked when the above requirements are no longer met. In other words, it must be ensured that the state of the ENUM domain name tracks any change in state and ownership of the

corresponding E.164 number. The regular process of checking that the above requirements are still satisfied is commonly called "recurring validation" or "revalidation".

The above requirements are usually part of the local registration policy issued by the authorities in charge of ENUM administration.

3. ENUM Provisioning Model and Roles

The above requirements lead to the introduction of a new role in the provisioning model, an entity performing validation related tasks: The Validation Entity (VE). A typical ENUM provisioning model, on which this document is based, is depicted in Figure 1:



Legend:

ASP: Application Service Provider
 DNS-SP: Domain Name System Service Provider
 NAE: Number Assignment Entity
 VE: Validation Entity

Figure 1: ENUM Model

These different roles are described further below. Note that an entity can act in more than one of these roles simultaneously; for example, the Registrar, the DNS-SP, and the ASP roles could be performed by a single company.

3.1. Number Assignment Entity (NAE)

A Number Assignment Entity (NAE) assigns E.164 numbers to end-users. Often, but not always, the Communication Service Provider (CSP) of the end-user (Assignee) acts as NAE. There are two main variants for E.164 number assignments:

1. Indirect assignment:

The National Number Plan Administrator (NNPA) assigns ranges of E.164 numbers to CSPs. Out of these ranges, the CSPs assign numbers (or number blocks) to their customers (end-users, Assignees). In this variant, the CSPs perform the role of the NAE.

2. Direct assignment:

In certain cases, an NNPA assigns E.164 numbers directly to Assignees (end-users), and therefore the NNPA acts as NAE in this variant. Typically, this concerns the assignment of special purpose numbers (e.g., premium rate).

These two variants of E.164 number assignment are depicted in Figure 2:

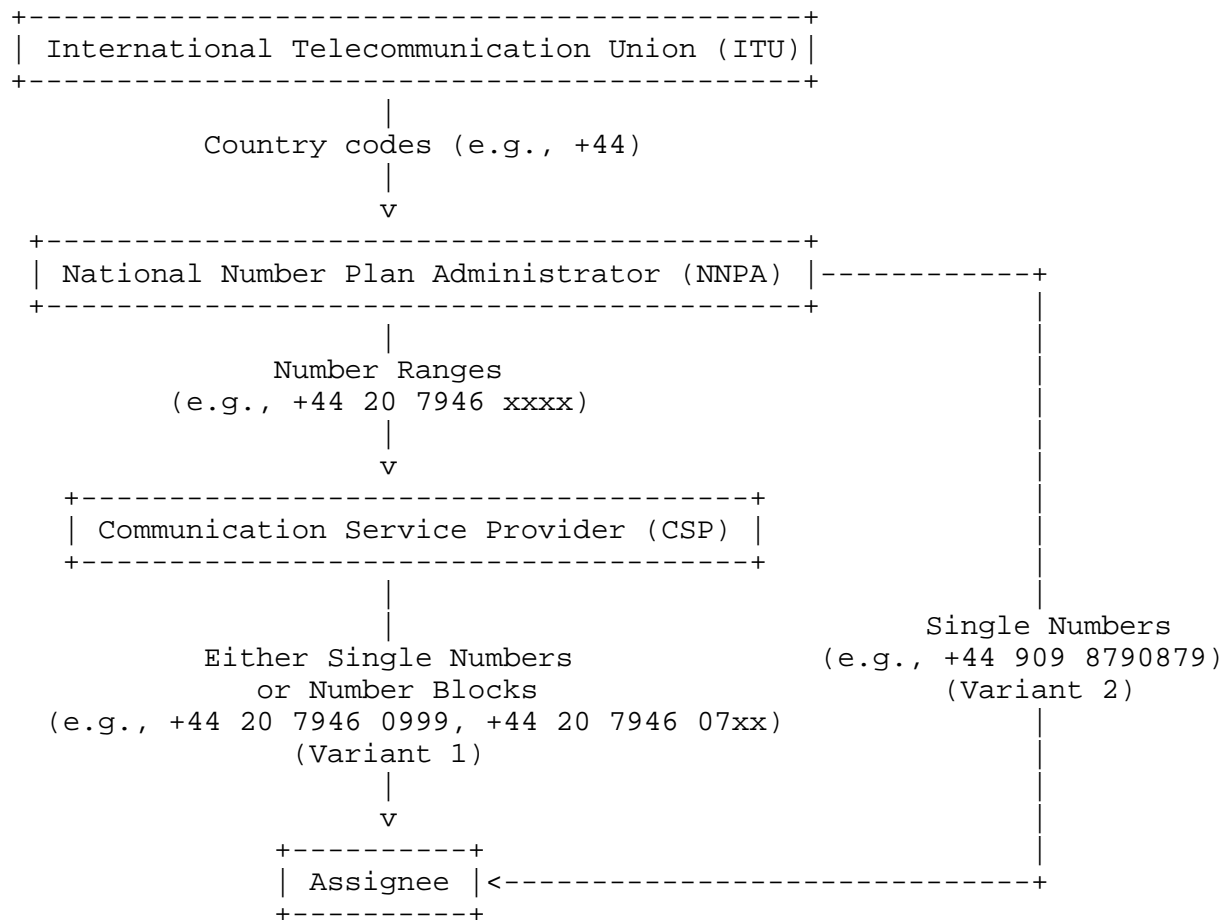


Figure 2: E.164 Number Assignment

(Note: Numbers above are "drama" numbers and are shown for illustrative purpose only. Assignment policies for similar "real" numbers in country code +44 may differ.)

As the Assignee (subscriber) data associated with an E.164 number is the primary source of number assignment information, the NAE usually holds the authoritative information required to confirm the assignment.

A CSP that acts as NAE (indirect assignment) may therefore easily assert the E.164 number assignment for its subscribers. In some cases, such CSPs operate database(s) containing service information on their subscribers' numbers. Typically, authorized entities such

as other CSPs are allowed to access these databases, in real-time, under contract for the limited purposes of billing and validation (no marketing, data mining, or otherwise). These databases could be re-used for ENUM validation purposes.

Number portability transactions may lead to situations where the CSP that originally acted as NAE no longer has authoritative assignment information about ported numbers. Whether the old and/or the new CSP act(s) as NAE for ported numbers depends on local policy.

However, it is unlikely that all CSPs acting as NAEs will participate in ENUM validation.

3.2. Assignee

The person or organization to whom a NAE assigns an E.164 number is called Assignee of this number. For the scope of this document, the terms Assignee, subscriber, and number-holder are used equivalently.

The Assignee has the "right to use" on the assigned E.164 number.

3.3. Registrant

The ENUM Registrant is the end-user, the person or organization who is the "holder" of the ENUM domain name.

The Registrant usually has control over his ENUM domain name(s) and its DNS zone content.

3.4. Validation Entity (VE)

The Validation Entity (VE) verifies whether or not the Registrant of an ENUM domain name is identical to the Assignee of the corresponding E.164 number.

Often it also verifies that the entity requesting the registration of an ENUM domain name is either the Assignee of the corresponding E.164 number itself or an entity authorized to request registration on behalf of said Assignee.

This role may be performed by several parties and is not necessarily limited to a single entity.

The actual validation methods applied may vary depending on, e.g., the particular party, available data sources, Assignee's choice, and regulatory requirements. Validation methods are out of scope of this document.

3.5. Registry

The ENUM Registry operates the master database of ENUM domain delegations and runs the authoritative nameservers for the relevant zone under e164.arpa. There must always be a single authoritative ENUM Registry for a specific zone.

3.6. Registrar

An ENUM Registrar performs ENUM domain delegations on behalf of a Registrant by interacting with the Registry, typically through a protocol like Extensible Provisioning Protocol (EPP) [5]. This role is similar to the one that Registrars fulfill in the "ordinary" domain name registration world.

The Registrar may well not be the same entity as the CSP of the Registrant. Therefore, a Registrar may lack authoritative number-assignment information. If the Registrar and the CSP are the same entity (or has a source of authoritative data), the Registrar could perform the role of the VE itself.

In any case, a Registrar has to ensure a proper validation through a VE prior to the registration of an ENUM domain name.

3.7. Domain Name System Service Provider (DNS-SP)

The Domain Name System Service Provider (DNS-SP) operates the nameservers for the ENUM DNS zones, which contain the ENUM Naming Authority Pointer (NAPTR) Resource Record (RR) entries [1].

In most cases, the Registry delegates the ENUM DNS zones to the nameservers at the DNS-SP.

The DNS-SP is usually not involved in the validation process.

3.8. Application Service Provider (ASP)

The Application Service Provider (ASP) operates a service for the Registrant. This service could be an IP telephony service, whereby the service provider populates the ENUM zone for its customers so that others can discover that customer's URI.

Usually, the ASP is not involved in the validation process.

4. Validation Process Assumptions

4.1. Workflow

The prototypical initial validation workflow using the above roles and definitions consists of the following steps:

1. A potential Registrant approaches a Registrar, and orders an ENUM domain name.
2. The Registrar chooses a cooperating Validation Entity, and requests an initial validation for the ENUM domain name ordered.
3. The Validation Entity performs the actual validation, which could require interaction with the Assignee/Registrant.
4. The Validation Entity indicates the result of the initial validation to the Registrar.
5. If the validation process was successful, the Registrar provisions the ENUM domain name with the Registry. Depending on the local Registry policy, validation-related information may be provided to the Registry along with this registration.

In most cases, local policy mandates expiration dates to be imposed on successful validations. If the ENUM delegation is to be kept beyond this expiration date, recurring validation has to be performed. A typical revalidation workflow involves the following steps:

1. In good time before the current validation expires, the Registrar requests the Validation Entity to revalidate the domain name in question.
2. The Validation Entity verifies if the delegation requirements are still met. It may use information acquired during the initial validation or associated to the registration data.
3. The Validation Entity indicates the result of the recurring validation to the Registrar.
4. In case the revalidation has been successful, the domain delegation may persist. Local Registry policy may require updating domain name registration data, especially in case the Registry keeps validation-related expiry information.

5. In case the revalidation has failed, the ENUM domain delegation must be suspended, either by explicit interaction with the Registry or -- if the Registry keeps validation-related information -- automatically when the current validation expires. Local policy may grant a grace period on the expiration date.

This workflow ensures the integrity between the E.164 and ENUM namespaces. ENUM domain delegations that fail to meet the validation requirements are suspended from the DNS.

4.2. Trust Relations

The above validation workflow implies the following trust relations:

- o The Registry trusts the Validation Entities to enforce the local validation policy.
- o The Registrars trust the Validation Entities to properly perform validation based on the Registrar's request.
- o Depending on the amount of validation data provided to the Registry additional trust relations may be necessary. Three cases can be differentiated:
 - * The Registry receives no validation-related data: The Registry needs to trust the Registrar that validation has been performed, and the result was positive. In addition, the Registry needs to trust the Registrar that it will properly remove delegations for which revalidation fails.
 - * The Registry receives validation-related data including expiry date, but there are no means of checking its authenticity: The Registry needs to trust the Registrar that the validation data provided is authentic.
 - * The Registry receives validation-related data including expiry date and means to verify its authenticity (e.g., a cryptographic signature issued by the VE): No additional trust relations are necessary.

4.3. Data Flow and Format

The validation process requires the following regular data flows (Note: data flows not directly related to validation are out of scope of this document):

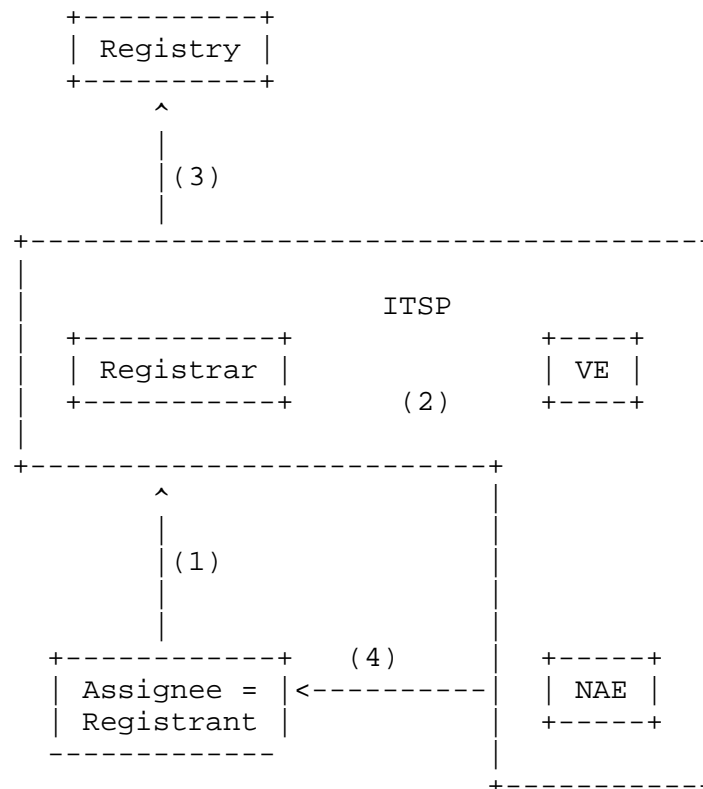
- o Registrars communicate with Validation Entities to initiate, modify, or cancel validation requests. Validation Entities act upon validation requests and provide validation results to Registrars. Since Registrars could potentially communicate with several Validation Entities, and Validation Entities could provide services to several Registrars (worst case: full mesh), a standardized protocol and data format should be used in this data flow.
- o If the local Registry policy mandates that validation-related information is to be stored along with delegation records, a validation-related data flow between Registry and Registrar is required. Since the registration itself already requires communication between those entities, validation-related information in a standardized data format should be embedded into the existing Registry-Registrar protocol data flow.
- o Validation Entities may need to communicate with Assignees to perform validation. A Validation Entity may choose to perform all communication with the Assignee via the requesting Registrar rather than contacting the Assignee by itself. Since the actual communication form and process are expected to greatly vary, it does not make sense to specify any data formats or processes for this purpose.

5. Example Scenarios

5.1. E.164 Number Assignment along with ENUM Registration

In this simple scenario, we assume that the roles of the Registrar, the VE, and the NAE are performed by the same entity, e.g., an Internet Telephony Service Provider (ITSP). This ITSP is a CSP that was assigned number ranges by the NNPA. Out of these ranges he assigns numbers to his customers (Assignees) to provide those with communication services. The ITSP chooses to assign an E.164 number together with the corresponding ENUM domain name. Therefore, it can perform the validation simply by reference to its subscriber database.

Figure 3 shows the external interactions needed for the ENUM domain name provisioning process:



Legend:

ITSP: Internet Telephony Service Provider
 NAE: Number Assignment Entity
 VE: Validation Entity

Figure 3: E.164 Number Assignment along with ENUM Registration

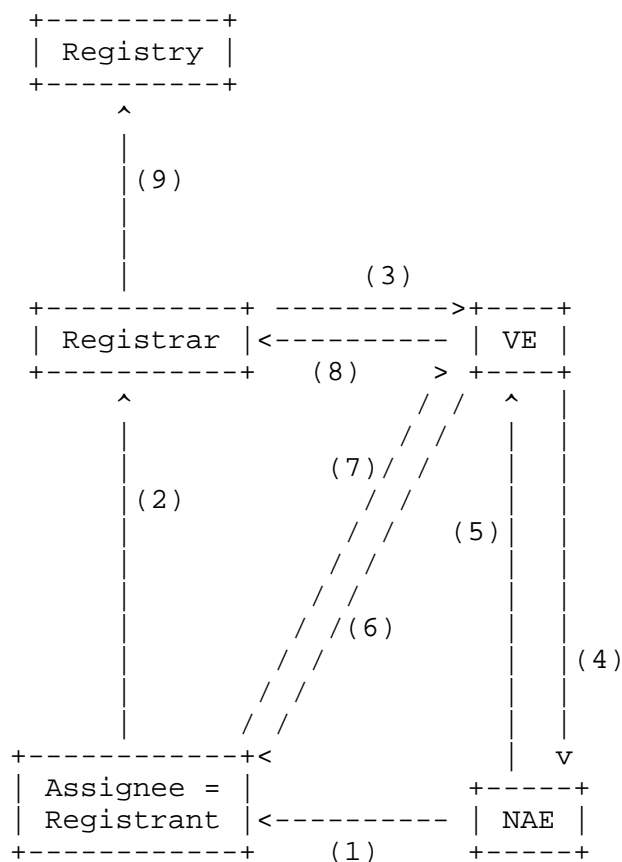
- (1) The ITSP receives an order for ENUM services.
- (2) The ITSP assigns a free E.164 number and performs the validation at the same time.
- (3) The ITSP sends an ENUM registration request to the Registry, which might contain additional information about the validation applied.
- (4) The ITSP sends a confirmation about the E.164 number assignment and the ENUM registration to its customer, who is now Assignee and Registrant.

This scenario is quite close to "ordinary" domain name registrations.

5.2. Fully Disjoint Roles

In this more complex scenario, we assume that all roles of the ENUM provisioning model are performed by different entities. In contrast with the previous example (in Section 5.1), we assume that the ENUM domain name to be registered is based on an already assigned E.164 number and the NAE in question provides the VE with access to the subscriber database. We further assume that there is a requirement for the VE to verify the intention of the Assignee. The validation process therefore involves also contacting the Assignee.

Figure 4 shows the interactions needed for the ENUM domain name provisioning process:



Legend:

NAE: Number Assignment Entity
VE: Validation Entity

Figure 4: Fully Disjoint Roles

- (1) The NAE assigns an E.164 number. This assignment could have been done long before the ENUM domain name registration, e.g., at the time when the Assignee subscribed to a common telephony service.
- (2) The Assignee orders the corresponding ENUM domain name at a Registrar of his choice.
- (3) The Registrar requests validation at an independent VE.
- (4) The VE contacts the subscriber database of the NAE, to verify that the Assignee of the E.164 number corresponds to the Registrant of the ENUM domain name.
- (5) The result of the NAE subscriber database is positive.
- (6) The VE performs a call-back to the E.164 number to be registered as ENUM domain name, makes provisions for authentication, and asks the Assignee to confirm his intention.
- (7) The Assignee confirms and the VE documents this confirmation.
- (8) The VE returns a positive answer to the Registrar. The answer might contain some additional information about the validation process, such as expiration date, validation method applied, and so on.
- (9) Finally, the Registrar sends an ENUM registration request to the Registry. Additional information about the validation process might be sent along with the registration request.

6. Security Considerations

6.1. Fraud Prevention

Situations where an entity has control over the ENUM domain of a third party's E.164 number impose high fraud potential. Unauthorized control over an ENUM domain of a bank could, for example, be used for "man in the middle" attacks on telephone banking applications. Cases of such attacks could discredit ENUM as a whole.

Implementing high-quality validation processes is therefore crucial to any ENUM deployment and should receive high attention.

6.2. Assignee Data

When handling Assignee data, privacy and discretion issues must be considered. Implementations transporting assignee data over the Internet must use authenticated and encrypted transport protocols. Local registration/validation policy and agreements should clearly limit usage of Assignee data.

7. Acknowledgements

The authors would like to thank the following persons for their valuable suggestions and contributions: Lawrence Conroy, Michael Haberler, Ted Hardie, Otmar Lendl, Hala Mowafy, Marcel Parodi, Jon Peterson, Penn Pfautz, Patrik Schaefer, and Richard Stastny.

8. References

8.1. Normative References

- [1] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.
- [2] ITU-T, "The international public telecommunication numbering plan", Recommendation E.164 (02/05), Feb 2005.

8.2. Informative References

- [3] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
- [4] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
- [5] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", RFC 3730, March 2004.

Authors' Addresses

Alexander Mayrhofer
enum.at GmbH
Karlsplatz 1/9
Wien A-1010
Austria

Phone: +43 1 5056416 34
EMail: alexander.mayrhofer@enum.at
URI: <http://www.enum.at/>

Bernie Hoeneisen
Switch
Neumuehlequai 6
CH-8001 Zuerich
Switzerland

Phone: +41 44 268 1515
EMail: hoeneisen@switch.ch, b.hoeneisen@ieee.org
URI: <http://www.switch.ch/>

Full Copyright Statement

Copyright (C) The IETF Trust (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST, AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

