

ENUM -- Telephone Number Mapping  
Working Group  
Internet-Draft  
Expires: January 9, 2006

O. Lendl  
enum.at  
July 8, 2005

**ENUM Validation Token Format Definition**  
**draft-lendl-enum-validation-token-00**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 9, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

An ENUM domain name is tightly coupled with the underlying E.164 number. The process of verifying whether 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 an signed XML data format -- the Validation Token -- with which Validation Entities can convey successful completion of a validation procedure in a secure fashion.

## Table of Contents

|                     |                                                          |                    |
|---------------------|----------------------------------------------------------|--------------------|
| <a href="#">1.</a>  | Introduction . . . . .                                   | <a href="#">3</a>  |
| <a href="#">2.</a>  | Data Requirements . . . . .                              | <a href="#">3</a>  |
| <a href="#">3.</a>  | Digital Signature . . . . .                              | <a href="#">3</a>  |
| <a href="#">4.</a>  | Field Descriptions . . . . .                             | <a href="#">4</a>  |
| <a href="#">4.1</a> | Mandatory Section . . . . .                              | <a href="#">4</a>  |
| <a href="#">4.2</a> | Optional Section . . . . .                               | <a href="#">5</a>  |
| <a href="#">5.</a>  | Examples . . . . .                                       | <a href="#">5</a>  |
| <a href="#">5.1</a> | Unsigned token without registrant information . . . . .  | <a href="#">5</a>  |
| <a href="#">5.2</a> | Unsigned token with registrant information . . . . .     | <a href="#">6</a>  |
| <a href="#">5.3</a> | Signed token . . . . .                                   | <a href="#">7</a>  |
| <a href="#">6.</a>  | Formal Syntax . . . . .                                  | <a href="#">9</a>  |
| <a href="#">6.1</a> | Token Core Schema . . . . .                              | <a href="#">9</a>  |
| <a href="#">6.2</a> | Token Data Schema . . . . .                              | <a href="#">11</a> |
| <a href="#">7.</a>  | Wider applicability . . . . .                            | <a href="#">13</a> |
| <a href="#">8.</a>  | Security Considerations . . . . .                        | <a href="#">13</a> |
| <a href="#">9.</a>  | Acknowledgements . . . . .                               | <a href="#">14</a> |
| <a href="#">10.</a> | References . . . . .                                     | <a href="#">14</a> |
|                     | Author's Address . . . . .                               | <a href="#">15</a> |
|                     | Intellectual Property and Copyright Statements . . . . . | <a href="#">16</a> |

Lend1

Expires January 9, 2006

[Page 2]

## **1. Introduction**

In most cases, the ENUM [2] domain should only be delegated to the assignee of the corresponding E.164 number. In the role model described in the architecture draft (work in progress) [9] the entity which performs this check is called the Validation Entity (VE).

The ENUM Validation Token is a signed XML [4] document with which the VEs can communicate to the registry over an untrusted path (i.e. the Registrar) that the validation issues for a specific delegation request have been taken care of.

## **2. Data Requirements**

As the data within the Token is the only communication between the VE and the registry, a Token needs at a minimum contain as much information as the Registry needs to grant the delegation of the requested ENUM domain. The registry itself does not care about the actual validation procedure details, it only needs to know that (a) an accredited VE has (b) recently (c) successfully validated a delegation request for (d) a specific registrar concerning (e) a specific E.164 number for (f) which time-span using (g) a specific approved method.

In addition to these necessary information, the Token can also contain data about the registrant which the VE has also ascertained during the validation procedure. This additional data about the number holder/registrar can be used to simplify the revalidation procedure.

For example, if the initial validation consists of the steps "Check the identity of the registrant" and "Check the ownership of a E.164 number" then a revalidation needs only check the second part again.

As the Token will be included in XML-based registry/registrar protocols like EPP it is a natural choice to use XML to encode Validation Tokens.

## **3. Digital Signature**

There is a trust relationship between the registry and the VE, but no direct, secured communication link. The Token will be submitted to the registry as part of the delegation request by the registrar who is not necessarily trusted by the registry regarding validation issues.

It is also possible that a VE does not directly talk with the registrar, but instead only interacts with the registrant and hands

Lend1

Expires January 9, 2006

[Page 3]

the Token to him.

Given these untrusted paths, the Token needs to be protected from tampering on its way from the VE to the registry. Furthermore, the registry needs to be sure that the Token was indeed created by the VE noted inside the Token.

A digital signature on the token guarantees that

- o the token was indeed generated by the indicated VE (authenticity)
- o the token was not tampered with in transit (integrity)
- o auditing the validation process is possible (non-repudiation).

The cryptographic signature on the token follows XML-DSIG [7]. As tokens might be transmitted as part of an already XML based protocol the transform as specified in [8] is used. In order to make the signature an integral part of the token the "enveloped"-signature mode is employed. The actual signature uses the RSA-SHA1 algorithm and relies on X.509 certificates. The signature covers all information contained in the Token.

This document does not assume a public key infrastructure. Whether the registry acts as a certificate authority, accepts certs from a public CA, or only accepts pre-registered keys is a local policy choice. Including certificates within the signature is recommended as this makes checking the signature possible without references to external information.

## **4. Field Descriptions**

### **4.1 Mandatory Section**

A token must contain a <validation> tag which contains the following:

- o A single validation "serial" string uniquely identifying a validation token for a certain VE.
- o A single "e164number" attribute, containing the E.164 number in international format for which validation was carried out.
- o A single "validator" id, identifying the VE.
- o A single "method" id, identifying the method used by the VE for validation.
- o A single "registrar" id, identifying the registrar for which validation was carried out.
- o A single "createdate" attribute, containing the date of validation, formatted as "full-date" according to RFC3339 [3].
- o A single "expiredate" attribute, marking the expiration date of the validation token, formatted as "full-date" according to RFC3339. This is the only optional attribute in this section. A missing expiredate signifies that this ENUM domain does not need to undergo regular revalidation procedures.

Lend1

Expires January 9, 2006

[Page 4]

## **4.2 Optional Section**

A token MAY contain a "tokendata" section. The section contains information about the entity whose right-to-use is being asserted.

- o A single "organization" attribute, containing the full name of the entity.
- o A single "commercialregisternumber" attribute, containing the entity's registration number.
- o A single "title" attribute.
- o A single "firstname" attribute.
- o A single "lastname" attribute.
- o A single "address" section, containing the following attributes:
  - \* A single mandatory "streetname" attribute
  - \* A single optional "streetnumber" attribute
  - \* A single optional "apartment" attribute
  - \* A single mandatory "postalcode" attribute
  - \* A single mandatory "city" attribute
  - \* A single optional "state" attribute
  - \* A single mandatory "country" attribute
- o up to 10 "phone" attributes, containing full E.164 numbers
- o up to 10 "fax" attributes, containing full E.164 numbers
- o up to 10 "email" attributes

Basically, all attributes are optional. In case an address section is used, several components are mandatory for conformance with the E.115 [1] recommendation. The reason for this is that "computerized directory assistance" accessible through the E.115 interface may be a source of validation information.

## **5. Examples**

### **5.1 Unsigned token without registrant information**

This is the basic Token without any information about the registrant and without the cryptographic signature.

Lend1

Expires January 9, 2006

[Page 5]

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="http://www.enum.at/rxsd/enum-token-1.1" Id="TOKEN"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    "http://www.enum.at/rxsd/enum-token-1.1 enum-token-1.1.xsd">
  <validation serial="1">
    <e164number>+431987654321</e164number>
    <validator>AcmeVE</validator>
    <registrarid>bigITSP</registrarid>
    <method>1</method>
    <createdate>2005-07-08</createdate>
    <expiredate>2006-01-01</expiredate>
  </validation>
</token>
```

## [5.2](#) Unsigned token with registrant information

Lend1

Expires January 9, 2006

[Page 6]

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="http://www.enum.at/rxsd/enum-token-1.1" Id="TOKEN"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    "http://www.enum.at/rxsd/enum-token-1.1 enum-token-1.1.xsd">
  <validation serial="1">
    <e164number>+431987654321</e164number>
    <validator>AcmeVE</validator>
    <registrarid>bigITSP</registrarid>
    <method>1</method>
    <createdate>2005-07-08</createdate>
    <expiredate>2006-01-01</expiredate>
  </validation>
  <tokendata xmlns="http://www.enum.at/rxsd/enum-tokendata-1.1"
    xsi:schemaLocation=
      "http://www.enum.at/rxsd/enum-tokendata-1.1 enum-tokendata-1.1.xsd">
    <contact>
      <organisation>Example Corp.</organisation>
      <firstname>Peter</firstname>
      <lastname>Mustermann</lastname>
      <address>
        <streetname>Elm Street</streetname>
        <streetnumber>3</streetnumber>
        <postalcode>1010</postalcode>
        <city>Wien</city>
        <country>AT</country>
      </address>
      <email>pm@example.com</email>
    </contact>
  </tokendata>
</token>
```

### 5.3 Signed token

This example uses an X.509 based signature which includes the certificate of the signing validation entity. Thus the validity of the signature can be verified without the need for a key-server.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="http://www.enum.at/rxsd/enum-token-1.1" Id="TOKEN"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    "http://www.enum.at/rxsd/enum-token-1.1 enum-token-1.1.xsd">
  <validation serial="1">
    <e164number>+431987654321</e164number>
```

Lend1

Expires January 9, 2006

[Page 7]

```
<validator>AcmeVE</validator>
<registrarid>bigITSP</registrarid>
<method>1</method>
<createdate>2005-07-08</createdate>
<expiredate>2006-01-01</expiredate>
</validation>
<tokendata xmlns="http://www.enum.at/rxsd/enum-tokendata-1.1"
xsi:schemaLocation=
"http://www.enum.at/rxsd/enum-tokendata-1.1 enum-tokendata-1.1.xsd">
  <contact>
    <organisation>Example Corp.</organisation>
    <firstname>Peter</firstname>
    <lastname>Mustermann</lastname>
    <address>
      <streetname>Elm Street</streetname>
      <streetnumber>3</streetnumber>
      <postalcode>1010</postalcode>
      <city>Wien</city>
      <country>AT</country>
    </address>
    <email>pm@example.com</email>
  </contact>
</tokendata>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm=
      "http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm=
      "http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <Reference URI="#TOKEN">
      <Transforms>
        <Transform Algorithm=
          "http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm=
          "http://www.w3.org/2001/10/xml-exc-c14n#" />
        <InclusiveNamespaces xmlns=
          "http://www.w3.org/2001/10/xml-exc-c14n#"
          PrefixList="enum-token enum-tokendata" />
      </Transforms>
    </Reference>
    <DigestMethod Algorithm=
      "http://www.w3.org/2000/09/xmldsig#sha1" />
    <DigestValue>gtgIo5RnM5i0fk0KxP8otc0/YrA=</DigestValue>
  </SignedInfo>
  <SignatureValue>WATnADceCRKMQU/
b9h4U8efoDe7zInxYj2+5R5aghKNy5pMYsCjV+2M8LxFyBJhk
z3fvw8ulheEcX0xj+Ih4qavbrmW9BgRWFPSiTSby+S2fm9zYjdWkCePuvxJUor89
```

w6lHYy1wGt2gCuXHfjv68uI/qD5HssxkSbmqALj9A8k=</SignatureValue>

Lend1

Expires January 9, 2006

[Page 8]

```
<KeyInfo>
<X509Data>
```

```
<X509Certificate>MIIDZjCCAs+gAwIBAgIBBDANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJBVDEP
MA0GA1UEBxMGVmllbm5hMRQwEgYDVQQKEwtCT0ZIIENlcnRzLjEhMBkGA1UEAxMS
Q0VSVFMuYm9maC5wcm12LmF0MSEwHwYJKoZIhvcNAQkBFhJjZXJ0c0Bib2ZoLnBy
aXYuYXQwHhcNMDQwNzIwMTMxNTA5WhcNMDUwNzIwMTMxNTA5WjB/MQswCQYDVQQG
EwJBVDEKMAgGA1UECBMLEPMA0GA1UEBxMGVmllbm5hMR0wGwYDVQQKEwRBY21l
IEVOVU0gVmFsaWRhdGlvbJEQMA4GA1UEAxMHYWNTZS1WRTEiMCAGCSqGSib3DQEJ
ARYTbm9ib2R5QGVudW0tYWNTZS5hdDCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkC
gYEAzJPcJmFc54/zwztSdQXGxUtodJT9r1qGI2lQPNjLvtPJg93+7o5SI0sZGSpg
zWbztDAV5qc7PHZWUVIyf6MbM5qSgQDVRjNRhTosNtyqmwi23BH52SKkX3P7eGit
LmqEkiUZRxZhZ6upRbtCqvKSwmXitvW4zXZhkVHYJZ2HuMcCAwEAAaOB/DCB+TAJ
BgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVYXRlZCBZDZlQ0
aWZpY2F0ZTAuBgNVHQ4EFgQUyK4otTQtvv6KdS1MB0PT5Ve18JgwgZ4GA1UdIwSB
ljCBk4AUvfPadpm0HhmZx2iAVumQTwnG2eheKR2MHQxCzAJBgNVBAYTAKFUMQ8w
DQYDVQQHEwZwawVubmExFDASBgNVBAoTC0JPRkggQ2VydHMuMRswGQYDVQQDEwJD
RVJUUYy5ib2ZoLnByaXYuYXQwITAFBgkqhkiG9w0BCQEWEmNlcnRzQGJvZmguYXQw
di5hdIIBADANBgkqhkiG9w0BAQQFAA0BgQCB9CHBnIUhrdic4h5Ar4hdxjHSQkDH
sJWd+MYrNcuSrv3TIOsUkUgNpNNhmKZPtixqfy3388IRdJtJiLWXSOb/XLZHOM9I
MvwKYwhcpQ9UdM/w7VpXQqf+CEj0XSyqxGw65UsHI0ijgiG/WyhSj+Lzriw7CTge
P2iAJkJVC4t2XA==
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</token>
```

## 6. Formal Syntax

The formal syntax of the validation token is specified using XML schema notation [5] [6]. Two schemas are defined: The "token core schema" contains mandatory attribute definitions, the "token data schema" defines the format of the optional "tokendata" section.

### 6.1 Token Core Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.enum.at/rxsd/enum-token-1.1"
  xmlns:enum-token="http://www.enum.at/rxsd/enum-token-1.1"
  xmlns:enum-tokendata="http://www.enum.at/rxsd/enum-tokendata-1.1"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">
```

Lend1

Expires January 9, 2006

[Page 9]

```
<!-- Import common element types. -->

<import namespace="http://www.w3.org/2000/09/xmldsig#"
      schemaLocation="xmldsig-core-schema.xsd"/>
<import namespace="http://www.enum.at/rxsd/enum-tokendata-1.1"
      schemaLocation="enum-tokendata-1.1.xsd"/>

<annotation>
  <documentation>
    enum.at Validation Token core schema
  </documentation>
</annotation>

<element name="token" type="enum-token:tokenBaseType"/>

<simpleType name="shortTokenType">
  <restriction base="token">
    <minLength value="1"/>
    <maxLength value="20"/>
  </restriction>
</simpleType>

<simpleType name="e164numberType">
  <restriction base="token">
    <maxLength value="64"/>
    <pattern value="\+\\s*\\d\\d\\s*[\\s\\d]{1,}" />
  </restriction>
</simpleType>

<complexType name="validationDataType">
  <sequence>
    <element name="e164number" type="enum-token:e164numberType"/>
    <element name="validator" type="enum-token:shortTokenType"/>
    <element name="registrarid" type="enum-token:shortTokenType"/>
    <element name="method" type="enum-token:shortTokenType"/>
    <element name="createdate" type="date"/>
    <element name="expiredate" type="date" minOccurs="0"/>
  </sequence>
  <attribute name="serial" type="enum-token:shortTokenType"
    use="required"/>
</complexType>

<complexType name="tokenBaseType">
  <sequence>
    <element name="validation" type="enum-token:validationDataType"/>
    <any namespace="http://www.enum.at/rxsd/enum-tokendata-1.1"
      minOccurs="0"/>
    <any namespace="http://www.w3.org/2000/09/xmldsig#" />
  </sequence>
</complexType>
```

Lend1

Expires January 9, 2006

[Page 10]

```
    </sequence>
    <attribute name="Id" type="ID" use="required"/>
  </complexType>

  <complexType name="infDataContainerType">
    <sequence>
      <element name="infData" type="enum-token:tokenBaseType"/>
    </sequence>
  </complexType>

</schema>
```

## **6.2 Token Data Schema**

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.enum.at/rxsd/enum-tokendata-1.1"
  xmlns:enum-tokendata="http://www.enum.at/rxsd/enum-tokendata-1.1"
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

  <annotation>
    <documentation>
      enum.at Validation Token tokendata schema.
    </documentation>
  </annotation>

  <element name="tokendata" type="enum-tokendata:tokenDataType"/>

  <simpleType name="streetNameType">
    <restriction base="token">
      <minLength value="1"/>
      <maxLength value="128"/>
    </restriction>
  </simpleType>

  <simpleType name="shortTokenType">
    <restriction base="token">
      <minLength value="1"/>
      <maxLength value="20"/>
    </restriction>
  </simpleType>

  <simpleType name="longTokenType">
    <restriction base="token">
      <minLength value="1"/>
```

Lend1

Expires January 9, 2006

[Page 11]

```
<maxLength value="64"/>
</restriction>
</simpleType>

<complexType name="addressType">
  <sequence>
    <element name="streetname" type="enum-tokendata:streetNameType"/>
    <element name="streetnumber" type="enum-tokendata:shortTokenType"
      minOccurs="0"/>
    <element name="apartment" type="enum-tokendata:shortTokenType"
      minOccurs="0"/>
    <element name="postalcode" type="enum-tokendata:shortTokenType"/>
    <element name="city" type="enum-tokendata:longTokenType"/>
    <element name="state" type="enum-tokendata:longTokenType"
      minOccurs="0"/>
    <element name="country" type="enum-tokendata:longTokenType"/>
  </sequence>
</complexType>

<group name="tokenContactBaseGroup">
  <sequence>
    <element name="organisation" type="enum-tokendata:shortTokenType"
      minOccurs="0"/>
    <element name="commercialregisternumber"
      type="enum-tokendata:shortTokenType" minOccurs="0"/>
    <element name="title" type="enum-tokendata:shortTokenType"
      minOccurs="0"/>
    <element name="firstname" type="enum-tokendata:longTokenType"
      minOccurs="0"/>
    <element name="lastname" type="enum-tokendata:longTokenType"
      minOccurs="0"/>
    <element name="address" type="enum-tokendata:addressType"
      minOccurs="0"/>
    <element name="phone" type="enum-tokendata:shortTokenType"
      minOccurs="0" maxOccurs="10" />
    <element name="fax" type="enum-tokendata:shortTokenType"
      minOccurs="0" maxOccurs="10" />
    <element name="email" type="enum-tokendata:shortTokenType"
      minOccurs="0" maxOccurs="10" />
  </sequence>
</group>

<complexType name="contactType">
  <sequence>
    <group ref="enum-tokendata:tokenContactBaseGroup"/>
  </sequence>
</complexType>
```

Lend1

Expires January 9, 2006

[Page 12]

```
<complexType name="tokenDataType">
  <sequence>
    <element name="contact" type="enum-tokendata:contactType"/>
  </sequence>
</complexType>

</schema>
```

## **7. Wider applicability**

The basic idea of this validation token can be helpful to other registries where any request for a delegation must be accompanied by a proof of ownership.

One example are all the specialized TLDs with strict rules on who qualifies for registering a domain under that TLD.

Even liberal TLDs could make use of validation tokens during a sunrise phase, where only applicants with a prior right to a name are allowed to register a domain.

Moving away from a the domain business, the telephone number portability verification needs to solve roughly the same validation problem as the ENUM domain delegation. A formalized system based on signed tokens could replace the manual process used in many countries.

## **8. Security Considerations**

The security of this Tokens depends on the security of the underlying XML DSIG algorithms. As such, all the security considerations from [7] apply here as well. Two points from there need special attention:

Transforms can be used to select the relevant data for signing and to discard irrelevant information (e.g. pretty-printing and name-space local names). They need to be selected with care.

The <Reference URI="#TOKEN"> element and attribute combined with the Id="TOKEN" attribute in <token> specifies that the signature should cover the complete token. Moving the Id="TOKEN" attribute to e.g. the <tokendata> tag would make the signature worthless.

It is thus critical that the registry does not only check whether the Token passes a generic XML-SEC signature check, but also that the signature uses approved transforms and references the <token> tag as well as that the certificate belongs to an accredited VE.

Lend1

Expires January 9, 2006

[Page 13]

The Token is not encrypted. If local policy dictates that the information contained within the token should be protected then this has to be handled via other means.

When processing a delegation request the registry needs to make sure that the information within the Token matches the delegation request. To avert replay attacks, local policy has to specify how long after "createdate" the Token remains valid.

## **9. Acknowledgements**

The author would like to thank the following persons for their valuable suggestions and contributions: Michael Haberler, Alexander Mayrhofer, Michael Braunoeder

## **10. References**

- [1] ITU-T, "Computerized Directory Assistance", Recommendation E.115, February 1995.
- [2] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", [RFC 3761](#), April 2004.
- [3] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", [RFC 3339](#), July 2002.
- [4] Paoli, J., Sperberg-McQueen, C., Bray, T., and E. Maler, "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C FirstEdition REC-xml-20001006, October 2000.
- [5] Maloney, M., Beech, D., Mendelsohn, N., and H. Thompson, "XML Schema Part 1: Structures", W3C REC REC-xmlschema-1-20010502, May 2001.
- [6] Malhotra, A. and P. Biron, "XML Schema Part 2: Datatypes", W3C REC REC-xmlschema-2-20010502, May 2001.
- [7] Solo, D., Reagle, J., and D. Eastlake, "XML-Signature Syntax and Processing", W3C REC REC-xmlsig-core-20020212, February 2002.
- [8] 3rd, D., Boyer, J., and J. Reagle, "Exclusive XML Canonicalization Version 1.0", W3C REC REC-xml-exc-c14n-20020718, July 2002.
- [9] Mayrhofer and Hoeneisen, "ENUM Validation Architecture", Internet drafts ([draft-mayrhofer-enum-validation-architecture-00.txt](#)),

Lend1

Expires January 9, 2006

[Page 14]

July 2005.

Author's Address

Otmar Lendl  
enum.at GmbH  
Karlsplatz 1/9  
Wien A-1010  
Austria

Phone: +43 1 5056416 33  
Email: [otmar.lendl@enum.at](mailto:otmar.lendl@enum.at)  
URI: <http://www.enum.at/>



## Intellectual Property Statement

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](mailto:ietf-ipr@ietf.org).

## Disclaimer of Validity

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 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.

## Copyright Statement

Copyright (C) The Internet Society (2005). 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.

## Acknowledgment

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

Lend1

Expires January 9, 2006

[Page 16]