Groupe de travail Réseau O. Lendl, enum.at
Request for Comments : 5105
Catégorie : Sur la voie de la normalisation décembre 2007
Traduction Claude Brière de L'Isle

Définition du format du jeton de validation ENUM

Résumé
Un nom de domaine ENUM est étroitement couplé au numéro E.164 sous-jacent. Le processur pour vérifier si l'enregistrant d'un nom de domaine ENUM est identique à l'allocataire du numéro E.164 correspondant est généralement appelé la "validation". Le présent document décrit un format de données XML signé -- le jeton de validation -- avec lequel les entités de validation peuvent mener à bien une procédure de validation de façon sécurisée.

Table des Matières

1. Introduction

Dans le cas où un nom de domaine ENUM (transposition de numéro E.164 [RFC3761]) correspond à un numéro E.164 existant [E.164], la délégation de ce domaine doit être autorisée par l'allocataire du numéro E.164 correspondant. Dans le modèle de rôle décrit dans la [RFC4725], l'entité qui effectue cette vérification est appelée l'entité de validation (VE, *Validation Entity*).

En portant un jeton de validation ENUM -- un document XML signé -- au registre, une VE certifie que les exigences de délégation ont été satisfaites et sont actuelles.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Exigences pour les données

Dans ce modèle, le jeton est le seul élément de données passé de la VE au registre. Donc, le jeton doit contenir au moins autant d'informations que ce qu'en exige le registre pour accorder la délégation du domaine ENUM demandé en accord avec sa politique d'enregistement. À ce titre, le registre va avoir besoin de la confirmation que :
- o le jeton a été créé par une VE accréditée,
- o la durée de validité du jeton se conforme à la politique,
- o la procédure de validation employée satisfait les exigences minimum établies par la politique,
- o et que le jeton est protégé contre les attaques d'altération et de répétition.

Au delà de ces informations obligatoires, le jeton peut facultativement inclure des informations sur le détenteur du numéro, en particulier, pour simplifier de futures revalidations.

Par exemple, si la validation initiale exige les étapes "Vérifier l'identité de l'enregistrant" et "Vérifier la possession d'un numéro E.164", alors une revalidation ultérieure a seulement besoin de revérifier la possession car l'identité de l'enregistrant ne change pas.

Comme le jeton va être inclus (voir par exemple, la [RFC5076]) dans les protocoles de registre/registraire fondés sur XML comme le protocole extensible d'approvisionnement (EPP, *Extensible Provisioning Protocol*) [RFC4930], c'est un choix naturel d'utiliser XML pour coder les jetons de validation.

3. Signature numérique

Conformément au modèle d'architecture, la propriété d'une délégation ENUM dépend de la relation de confiance entre le registre et la VE. En général, une liaison non de confiance entre le registre et la VE devrait être supposée (par exemple, le jeton est passé avec la demande d'enregistrement par un registraire, qui peut n'avoir aucun rôle dans l'affirmation du droit d'utilisation). Donc, le jeton doit être protégé contre la falsification, l'altération, et les attaques en répétition.

Une signature numérique sur le jeton :
- o affirme que le jeton a bien été généré par la VE indiquée (authenticité) ;
- o garantit que le jeton n'a pas été altéré dans le transit (intégrité) ;
- o permet un examen du processus de validation (non répudiation).

La signature cryptographique sur le jeton suit XML-DSIG [RFC3275]. Comme les jetons pourraient être transmis au titre d'un protocole déjà fondé sur XML, la canonisation XML exclusive [XML-CANO] DOIT être utilisée. Cette transformation garantit que les déclarations d'espace de noms héritées de l'XML environnant n'invalident pas la signature. Afin de faire de la signature une partie intégrante du jeton, le mode de signature "enveloppée" est employé. La signature couvre toutes les informations contenues dans le jeton.

XML-DSIG offre un certain nombre d'algorithmes cryptographiques pour résumer et signer les documents et recommande SHA1/RSA-SHA1. De récentes avancées en cryptanalyse ont répandu des doutes sur la sécurité de SHA1, rendant donc cette recommandation obsolète (voir par exemple les considérations sur la sécurité de la [RFC4055]). La [RFC4051] définit comment des algorithmes supplémentaires peuvent être utilisés avec XML-DSIG.

Les entités de validation DOIVENT être capables de signer les jetons conformément à XML-DSIG, DOIVENT prendre en charge RSA-SHA1 et RSA-SHA256 [RFC4051], DOIVENT prendre en charge les tailles de clés RSA de 1024 et 2048 bits, et DOIVENT être capables d'incorporer des certificats X.509 [X.509]. Le registre DOIT définir quels algorithmes de signature et tailles de clés il va accepter dans les jetons de validation au titre de sa politique locale.

Le choix de signatures fondées sur RSA n'exige pas d'infrastructure de clé publique. Que le registre agisse comme autorité de certification, accepte des certificats d'une autorité de certification publique, ou n'accepte que des clés pré-enregistrées est un choix de politique locale.

4. Description des champs

Le jeton de validation est structuré en trois parties : les informations de validation de base, les informations supplémentaires sur l'enregistrant, et la signature numérique. Le schéma XML se trouve à la Section 6.

4.1 Élément <validation>

Un jeton DOIT contenir un élément <validation> qui contient ce qui suit :

- Un seul attribut de validation "serial" identifiant un jeton de validation pour une certaine VE. Il doit être unique par VE.
- Un seul élément <E164Number> contenant le numéro E.164 sous-jacent en format pleinement qualifié (international).
- Un élément facultatif <lastE164Number>. Si il est présent, il indique que tout le bloc de numéro commençant par <E164Number> jusque et y inclus <lastE164Number> a été validé. Pour éviter des ambiguïtés, les deux numéros DOIVENT être de la même longueur.
- Un seul élément <validationEntityID> identifiant la VE.
- Un seul élément <registrarID> identifiant le registraire au nom duquel la validation a été effectuée.
- Un seul élément <methodID> identifiant la méthode utilisée par la VE pour la validation.
- Un seul attribut <executionDate> contenant la date de validation formatée comme "full-date" conformément à la [RFC3339].
- Un attribut facultatif <expirationDate> marquant la date d'expiration du jeton de validation, formaté comme "full-date" conformément à la [RFC3339]. Le registre va automatiquement révoquer la délégation à cette date sauf si un nouveau jeton a été soumis qui étend la durée de vie de la validation. Une <expirationDate> manquante indique une validité infinie du jeton.

Le format et les contraintes d'unicité de ces identifiants sont laissés à la politique locale du registre.

4.2 Élément <tokendata>

Un jeton peut contenir une section <tokendata> contenant des informations sur le détenteur du numéro, consistant en les éléments suivants :

- Un seul élément <organization> contenant le nom complet de l'organisation à laquelle l'enregistrant est affilié.
- Un seul élément <commercialregisternumber>. Si l'enregistrant est une société, alors ce champ peut être utilisé pour identifier de façon univoque cette société par son numéro d'enregistrement officiel dans le pays local. L'interprétation de ce champ est donc spécifique du pays.
- Un seul élément <title>.
- Un seul élément <firstname>.
- Un seul élément <lastname>.
- Une seule section <address> contenant les éléments suivants :
  - Un seul élément facultatif <streetName>
  - Un seul élément facultatif <houseNumber>
  - Un seul élément facultatif <postalCode>
  - Un seul élément facultatif <locality>
  - Un seul élément facultatif <countyStateOrProvince>
  - Un seul élément facultatif <ISOcountryCode>
- Jusqu'à 10 éléments <phone> contenant des numéros E.164 complets.
- Jusqu'à 10 éléments <fax> contenant des numéros E.164 complets.
- Jusqu'à 10 éléments <email>.

Tous les éléments directement en dessous de <tokendata> sont facultatifs. L'élément <ISOcountryCode> spécifie le pays en utilisant le code de pays à deux lettres provenant de la norme ISO 3166-1:2006 [ISO3166] (incluant ses mises à jour publiées par l'Agence de Maintenance 3166). La définition des cinq premiers éléments au sein de l'élément <address> se conforme à la seconde version de "Assistance à l'Annuaire par ordinateur" [E.115].

5. Exemples

5.1 Jeton non signé sans information de l'enregistrant

Ce jeton de base sans aucune information sur l'enregistrant et sans la signature cryptographique montre la disposition de base du jeton.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="urn:ietf:params:xml:ns:enum-token-1.0" Id="TOKEN"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation=
 "urn:ietf:params:xml:ns:enum-token-1.0 enum-token-1.0.xsd">
  <validation serial="acmeve-000002">
    <E164Number>+442079460200</E164Number>
   <lastE164Number>+442079460499</lastE164Number>
```

```
   <validationEntityID>ACME-VE</validationEntityID>
   <registrarID>reg-4711</registrarID>
   <methodID>42</methodID>
   <executionDate>2007-05-08</executionDate>
   <expirationDate>2007-11-01</expirationDate>
  </validation>
</token>
```

5.2 Jeton signé

Cet exemple utilise une signature fondée sur X.509 qui inclut le certificat de l'entité de validation signataire. Donc, la validité de la signature peut être vérifiée sans qu'il soit besoin d'un serveur de clés. Une signature valide est une condition nécessaire, mais pas suffisante, pour un jeton valide. Toute entité qui évalue un jeton a besoin de vérifier aussi d'autres facteurs, par exemple, le certificat et le schéma XML.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="urn:ietf:params:xml:ns:enum-token-1.0" Id="TOKEN"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:enum-token-1.0 enum-token-1.0.xsd">
  <validation serial="acmeve-000001">
   <E164Number>+442079460123</E164Number>
   <validationEntityID>ACME-VE</validationEntityID>
   <registrarID>reg-4711</registrarID>
   <methodID>42</methodID>
   <executionDate>2007-05-08</executionDate>
  </validation>
  <tokendata xmlns="urn:ietf:params:xml:ns:enum-tokendata-1.0"
   xsi:schemaLocation="urn:ietf:params:xml:ns:enum-tokendata-1.0 enum-tokendata-1.0.xsd">

   <contact>
    <organisation>Example Inc.</organisation>
    <commercialregisternumber>4711</commercialregisternumber>
    <title>Dr.</title>
    <firstname>Max</firstname>
    <lastname>Mustermann</lastname>
    <address>
     <streetName>Main</streetName>
     <houseNumber>10</houseNumber>
     <postalCode>1010</postalCode>
     <locality>London</locality>
     <countyStateOrProvince>London</countyStateOrProvince>
     <ISOcountryCode>GB</ISOcountryCode>
    </address>
    <phone>+442079460123</phone>
    <email>mm@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/2001/04/xmldsig-more#rsa-sha256"/>
    <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"/>
        </Transform>
      </Transforms>
      <DigestMethod
       Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue
      >VxqsBxSNPFwPAUlCHts3g3DehcexnB1dqUz+GypLZ0k=</DigestValue>
    </Reference>
  </SignedInfo>
<SignatureValue>QKqphKRNPokVZFbenje+HZZV+RLrNweGnlWBw7ngAtH+rtuslR8LhMLmC4DlBb9VHvKItl+7zLG
m3VgYsqfHH8q3jCl1mFxUIuLlIPqtpJs+xAHAJDzZ+vmsF/q2IgrSK0uMmKuU5V1gydDBOvIipcJx+PrPYyXYZSjQXk
WknK8=</SignatureValue>
 <KeyInfo>
<X509Data>
<X509Certificate>
MIIDZjCCAs+gAwIBAgIBBDANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJBVDEPMA0GA1UEBxMGVml
lbm5hMRQwEgYDVQQKEwtCT0ZIIENlcnRzLjEbMBkGA1UEAxMSQ0VSVFMuYm9maC5wcml2LmF0MSEwHwYJ
KoZIhvcNAQkBFhJjZXJ0c0Bib2ZoLnByaXYuYXQwHhcNMDQwNzIwMTMxNTA5WhcNMDUwNzIwMTMxNTA5
WjB/MQswCQYDVQQGEwJBVDEKMAgGA1UECBMBLTEPMA0GA1UEBxMGVmllbm5hMR0wGwYDVQQKExR
BY21lIEVOVU0gVmFsaWRhdGlvbjEQMA4GA1UEAxMHYWNtZS1WRTEiMCAGCSqGSIb3DQEJARYTbm9ib2R5
QGVudW0tYWNtZS5hdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArJPcjMFc54/zwztSdQXGxUtodJT9r1
qGI2lQPNjLvtPJg93+7o5SIOsZGSpgzWbztDAV5qc7PHZWUVIyf6MbM5qSgQDVrjNRhTosNtyqmwi23BH52SKkX3P
7eGitLmqEkiUZRxZhZ6upRbtcqvKSwmXitvW4zXZhkVHYJZ2HuMcCAwEAAaOB/DCB+TAJBgNVHRMEAjAAMC
wGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUyK4otTQ
tvv6KdSlMBOPT5Ve18JgwgZ4GA1UdIwSBljCBk4AUvfPadpm0HhmZx2iAVumQTwgnG2eheKR2MHQxCzAJBgNVB
AYTAkFUMQ8wDQYDVQQHEwZWaWVubmExFDASBgNVBAoTC0JPRkggQ2VydHMuMRswGQYDVQQDExJDR
VJUUy5ib2ZoLnByaXYuYXQxITAfBgkqhkiG9w0BCQEWEmNlcnRzQGJvZmgucHJpdi5hdIIBADANBgkqhkiG9w0B
AQQFAAOBgQCB9CHBnIUhrdic4h5Ar4hdxjHSQkDHsJWd+MYrNcuSrv3TIOsUkUgNpNNhmkZPtiXqfy3388IRdJtJiL
WXSOb/XlZHOM9IMvwKYwhcpQ9UdM/w7VpXQqf+CEj0XSyqxGw65UsHIOijgiG/WyhSj+Lzriw7CTgeP2iAJkJVC4t
2XA==
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</token>
```

6. Syntaxe formelle

La syntaxe formelle du jeton de validation est spécifiée en utilisant la notation de schéma XML [XML1] [XML2]. Deux schémas sont définis : le "schéma central de jeton" contient des définitions d'attribut obligatoires, et le "schéma de données de jeton" définit le format de la section facultative "tokendata". Les étiquettes "DÉBUT" et "FIN" ne font pas partie du schéma ; elles sont utilisées pour noter le début et la fin du schéma pour les besoins d'enregistrement d'URI.

6.1 Schéma central de jeton

DÉBUT

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

<schema targetNamespace="urn:ietf:params:xml:ns:enum-token-1.0"
  xmlns:enum-token="urn:ietf:params:xml:ns:enum-token-1.0"
  xmlns:enum-tokendata="urn:ietf:params:xml:ns:enum-tokendata-1.0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

<!--  Importe les types d'éléments communs.  -->

  <import namespace="http://www.w3.org/2000/09/xmldsig#"
       schemaLocation="xmldsig-core-schema.xsd"/>
  <import namespace="urn:ietf:params:xml:ns:enum-tokendata-1.0"
```

```
        schemaLocation="enum-tokendata-1.0.xsd"/>

    <annotation>
     <documentation>
      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="20"/>
      <pattern value="\+\d\d*"/>
     </restriction>
    </simpleType>

    <complexType name="validationDataType">
     <sequence>
      <element name="E164Number"
               type="enum-token:e164numberType"/>
      <element name="lastE164Number" minOccurs="0"
               type="enum-token:e164numberType"/>
      <element name="validationEntityID"
               type="enum-token:shortTokenType"/>
      <element name="registrarID"
               type="enum-token:shortTokenType"/>
      <element name="methodID"
               type="enum-token:shortTokenType"/>
      <element name="executionDate" type="date"/>
      <element name="expirationDate"
               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="urn:ietf:params:xml:ns:enum-tokendata-1.0"
       minOccurs="0"/>
      <any namespace="http://www.w3.org/2000/09/xmldsig#"/>
     </sequence>
     <attribute name="Id" type="ID" use="required"/>
    </complexType>
  </schema>
FIN
```

6.2 Schéma de données de jeton

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

```
<schema targetNamespace="urn:ietf:params:xml:ns:enum-tokendata-1.0"
 xmlns:enum-tokendata="urn:ietf:params:xml:ns:enum-tokendata-1.0"
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified">

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

 <simpleType name="E115String">
  <restriction base="string">
<pattern value="[&#x20;-&#x7A; -&#xD7FF;&#xE000;-&#xFFFD;]*"/>
  </restriction>
 </simpleType>

 <simpleType name="E115StringUb256">
  <restriction base="enum-tokendata:E115String">
   <minLength value="1"/>
   <maxLength value="256"/>
  </restriction>
 </simpleType>
 <simpleType name="countryCodeType">
  <restriction base="token">
   <minLength value="2"/>
   <maxLength value="2"/>
  </restriction>
 </simpleType>

 <simpleType name="TokenType">
  <restriction base="token">
   <minLength value="1"/>
   <maxLength value="64"/>
  </restriction>
 </simpleType>

 <complexType name="addressType">
  <all>
   <element name="streetName"     minOccurs="0"
    type="enum-tokendata:E115StringUb256" />
   <element name="houseNumber"    minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="postalCode"     minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="locality"       minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="countyStateOrProvince" minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="ISOcountryCode" minOccurs="0"
    type="enum-tokendata:countryCodeType"/>
  </all>
 </complexType>

 <group name="tokenContactBaseGroup">
  <sequence>
   <element name="organisation"  minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="commercialregisternumber" minOccurs="0"
    type="enum-tokendata:TokenType"/>
   <element name="title"        minOccurs="0"
    type="enum-tokendata:TokenType"/>
   <element name="firstname"     minOccurs="0"
    type="enum-tokendata:E115StringUb256"/>
   <element name="lastname"      minOccurs="0"
```

```
        type="enum-tokendata:E115StringUb256"/>
       <element name="address"       minOccurs="0"
        type="enum-tokendata:addressType"/>

       <element name="phone" type="enum-tokendata:TokenType"
        minOccurs="0" maxOccurs="10" />
       <element name="fax"   type="enum-tokendata:TokenType"
        minOccurs="0" maxOccurs="10" />
       <element name="email" type="enum-tokendata:TokenType"
        minOccurs="0" maxOccurs="10" />
     </sequence>
   </group>

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

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

  </schema>
FIN
```

7. Autres applications du concept de jeton

Le concept de jeton de validation peut être utile dans d'autres applications de type registre où la preuve d'un droit sous-jacent est une condition d'un enregistrement valide.

Un exemple est celui d'un domaine de niveau supérieur où l'enregistrement est soumis à la preuve d'une certaine précondition, comme une marque commerciale ou le droit à un nom. De telles situations surviennent souvent durant l'introduction d'un nouveau domaine de niveau supérieur, par exemple, durant une phase de "lever de soleil".

Une base de données de portabilité de numéros (NP, *Number Portability*) fait face à des problèmes très similaires de vérification. Un système NP fondé sur le concept de jeton pourrait éventuellement être supérieur aux méthodes courantes, et aider à la convergence de NP et ENUM.

8. Considérations relatives à l'IANA

Le présent document utilise des noms de ressources universelles (URN, *Uniform Resource Name*) pour décrire les espaces de noms XML et les schémas XML qui se conforment à un mécanisme de registre décrit dans la [RFC3688]. L'IANA a fait les quatre allocations d'URI suivantes.

1. Enregistrement pour l'espace de noms de jeton :
   * URI : urn:ietf:params:xml:ns:enum-token-1.0
   * Contact d'enregistrant : voir la section "Adresse de l'auteur" de ce document.
   * XML : aucun. Les URI d'espace de noms ne représentent pas une spécification XML.

2. Enregistrement pour le schéma XML token :
   * URI: urn:ietf:params:xml:schema:enum-token-1.0
   * Contact d'enregistrant : voir la section "Adresse de l'auteur" de ce document.
   * XML: voir le paragraphe 6.1 de ce document.

3. Enregistrement pour l'espace de noms de données de jeton :
   * URI: urn:ietf:params:xml:ns:enum-tokendata-1.0

* Contact d'enregistrant : voir la section "Adresse de l'auteur" de ce document.
* XML : aucun. Les URI d'espace de noms ne représentent pas une spécification XML.

4. Enregistrement pour le schéma XML tokendata :
   * URI: urn:ietf:params:xml:schema:enum-tokendata-1.0
   * Contact d'enregistrant : voir la section "Adresse de l'auteur" de ce document.
   * XML : voir le paragraphe 6.2 de ce document.

Les identifiants utilisés dans les éléments validationEntityID, RegistrarID, et methodID sont soumis à la politique locale et n'exigent donc pas d'enregistrement par l'IANA.

9. Considérations sur la sécurité

La sécurité du jeton de validation dépend de la sécurité des algorihmes XML DSIG sous-jacents. À ce titre, toutes les considérations sur la sécurité provenant de la [RFC3275] s'appliquent aussi ici. Deux points de la [RFC3275] méritent d'être répétés :

Les transformations sont utilisées pour choisir les données pertinentes pour signer et éliminer les informations non pertinentes (par exemple, les noms locaux d'impression et d'espace de noms).

L'élément et l'attribut <Reference URI="#TOKEN"> combinés avec l'attribut Id="TOKEN" dans <token> spécifient que la signature devrait couvrir le jeton complet. Déplacer l'attribut Id="TOKEN" à, par exemple, l'élément <tokendata> rendrait la signature sans valeur.

Il est donc critique que le registre vérifie non seulement si le jeton est accepté par une vérification générique XML-DSIG de signature, mais aussi que :
1. la signature utilise des transformations et des algorithmes cryptographiques approuvés ;
2. la signature fait référence à l'élément <token> ;
3. la clé utilisée dans la signature appartient à une VE accréditée.

Le contenu du jeton n'est pas chiffré. Si la politique locale impose que les informations contenues dans le jeton soient confidentielles, alors cela doit être traité par un mécanisme différent.

Quand il traite une demande de délégation, le registre DOIT vérifier que les informations contenues dans le jeton correspondent à la demande de délégation. L'élément <registrarID> dans le jeton empêche un second registraire malveillant d'utiliser un jeton espion pour enregistrer un domaine dans son nom. Le registre DOIT vérifier que l'élément <expirationDate> donné (y compris dans le cas où aucune date d'expiration n'est donnée) se conforme à la politique du registre. Pour avertir des attaques en répétition, la politique locale DOIT spécifier pendant combien de temps après <executionDate> le jeton peut être utilisé pour autoriser une délégation.

10. Remerciements

L'auteur tient à remercier les personnes suivantes de leurs précieuses suggestions et contributions : Michael Haberler, Alexander Mayrhofer, Bernie Hoeneisen, Michael Braunoeder, Staffan Hagnell, Lawrence Conroy, et Tony Rutkowski.

11. Références

11.1 Références normatives

[E.164] Recommandation UIT-T E.164, "Plan de numérotation des télécommunication internationales publiques", UIT-T, Genève, février 2005.

[ISO3166] Organisation Internationale de normalisation, "Codes pour la représentation des noms de pays et de leurs subdivisions -- Partie 1 : Codes de pays, 2ième édition", Norme ISO 3166, novembre 2006.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3275] D. Eastlake 3rd , J. Reagle, D. Solo, "Syntaxe et traitement de signature en langage de balisage extensible (XML)", mars 2002. *(D.S.)*

[RFC3339] G. Klyne, C. Newman, "La date et l'heure sur l'Internet : horodatages", juillet 2002. *(P.S.)*

[RFC3688] M. Mealling, "Registre XML de l'IETF", BCP 81, janvier 2004.

[RFC3761] P. Faltstrom, M. Mealling, "Application de E.164 au système de découverte dynamique de délégation (DDDS) d'identifiants de ressource uniformes (URI) (ENUM)", avril 2004. *(P.S.) (Obsolète, voir la* RFC6116)

[RFC4051] D. Eastlake 3rd, "Identifiants de ressource universels (URI) de sécurité supplémentaires en XML", avril 2005. *(P.S.) (Remplacée par* RFC6931)

[XML1] Maloney, M., Beech, D., Mendelsohn, N., and H. Thompson, "XML Schema Part 1: Structures", W3C REC REC-xmlschema-1-20010502, mai 2001.

[XML2] Malhotra, A. and P. Biron, "XML Schema Part 2: Datatypes", W3C REC REC-xmlschema-2-20010502, mai 2001.

[XML-CANO] Eastlake, D., Boyer, J., and J. Reagle, "Exclusive XML Canonicalization Version 1.0", W3C REC REC-xml-exc-c14n-20020718, juillet 2002.

[X.509] Union Internationale des Télécommunications, "Technologie de l'information - Interconnexion des systèmes ouverts - L'Annuaire : cadres de clé publique et de certificat d'attribut", Recommandation UIT-T X.509, Norme ISO 9594-8, mars 2000.

11.2 Références pour information

[E.115] Recommandation UIT-T E.115v2, "Assistance à l'Annuaire par ordinateur, version 2", octobre 2005.

[RFC4055] J. Schaad et autres, "Algorithmes et identifiants supplémentaires pour la cryptographie RSA à utiliser dans le profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", juin 2005.

[RFC4725] A. Mayrhofer, B. Hoeneisen, "Architecture de validation pour ENUM", novembre 2006. *(Information)*

[RFC4930] S. Hollenbeck, "Protocole d'approvisionnement extensible (EPP)", mai 2007. *(D.S., remplacée par la* RFC5730)

[RFC5076] B. Hoeneisen, "Transposition d'informations de validation d'ENUM pour le protocole d'approvisionnement extensible", décembre 2007. *(P.S.)*

Adresse de l'auteur

Otmar Lendl
enum.at GmbH
Karlsplatz 1/2/9
Wien A-1010
Austria

téléphone : +43 1 5056416 33
mél : otmar.lendl@enum.at
URI : http://www.enum.at/

Déclaration complète de droits de reproduction