Groupe de travail Réseau
Request for Comments : 4991
Catégorie : sur la voie de la normalisation

A. Newton, VeriSign, Inc.
août 2007
Traduction Claude Brière de L'Isle

Schéma commun pour les protocoles de transfert de service d'information de registre Internet

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
(La présente traduction incorpore les errata 2285 et 1011)

Résumé
Le présent document décrit un schéma XML à utiliser dans les protocoles de transfert d'application de service d'informations de registre Internet (IRIS, *Internet Registry Information Service*) qui partagent des caractéristiques communes. Il décrit les informations communes sur le protocole de transfert, comme la version, les extensions prises en charge, et les mécanismes de sécurité acceptés.

Table des Matières

1. Introduction

IRIS [RFC3981] possède deux protocoles de transfert, LWZ *(lightweight using compression)* [RFC4993] et XPC (*XML pipelining with chunks)* [RFC4992], qui partagent des mécanismes de négociation communs. Les deux protocoles de transfert nécessitent que le serveur fournisse des informations d'état détaillées aux clients pendant la négociation du protocole. Dans de nombreux cas, ces informations d'état seraient trop complexes pour être décrites à l'aide de simples champs de bits et de séquences d'octets de longueur spécifiée. Le présent document définit un schéma XML pour ces informations d'état détaillées et décrit l'utilisation d'un XML conforme pour porter ces informations d'état.

Le présent document définit cinq types d'informations utilisées dans la négociation des capacités du protocole : version, taille, succès de l'authentification, échec de l'authentification, et autres informations. Les informations de version sont utilisées pour négocier les versions et les extensions du protocole de transfert, le protocole des opérations d'application et les modèles de données utilisés par les opérations d'application. Les informations de taille sont utilisées pour indiquer les

capacités et les erreurs de taille des demandes et des réponses. Les informations de succès et d'échec de l'authentification sont utilisées pour indiquer le résultat d'une action d'authentification. Des autres types d'informations peuvent aussi être transmis, qui résultent généralement d'une erreur mais ne peuvent pas être corrigés par le comportement défini du protocole.

Par exemple, à l'initialisation d'une connexion, un serveur peut envoyer des informations de version informant le client des modèles de données pris en charge par le serveur et des mécanismes de sécurité pris en charge par le serveur. Le client peut alors répondre de manière appropriée. Par exemple, le client peut ne reconnaître aucun des modèles de données pris en charge par le serveur et donc fermer la connexion. En revanche, le client peut reconnaître les modèles de données et les mécanismes de sécurité et commencer la procédure d'initialisation d'un mécanisme de sécurité avec le serveur avant de procéder à l'interrogation des données selon un modèle de données reconnu.

LWZ [RFC4993] et XPC [RFC4992] fournissent tous deux des exemples de l'utilisation du schéma XML défini dans le présent document.

2. Terminologie utilisée dans le document

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].

3. Syntaxe XML formelle

Voici le schéma XML utilisé pour définir les informations d'état de protocole de transfert. Voir les spécifications suivantes : [XML], [XML-Esp], [XML-Data], [XML-Str]. Les mises à jour ou changements à ce schéma exigent un document qui METTE À JOUR ou rende OBSOLÈTE le présent document.

```
<?xml version="1.0"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
      xmlns:iristrans="urn:ietf:params:xml:ns:iris-transport"
      targetNamespace="urn:ietf:params:xml:ns:iris-transport"
      elementFormDefault="qualified" >

<annotation>
 <documentation>
   Schéma pour décrire les information détat à utiliser par plusieurs protocoles de transfert.
 </documentation>
</annotation>

<element name="versions">
 <complexType>
  <sequence>
   <element name="transferProtocol" maxOccurs="unbounded">
    <complexType>
     <sequence>
      <element name="application" minOccurs="0" maxOccurs="unbounded">
       <complexType>
        <sequence>
         <element name="dataModel" minOccurs="0" maxOccurs="unbounded">
          <complexType>
           <attribute name="protocolId" type="token" use="required" />
           <attribute name="extensionIds" type="normalizedString" />
          </complexType>
         </element>
        </sequence>
        <attribute name="protocolId" type="token" use="required" />
        <attribute name="extensionIds" type="normalizedString" />
       </complexType>
```

```
          </element>
        </sequence>
       <attribute name="protocolId" type="token" use="required" />
        <attribute name="extensionIds" type="normalizedString" />
        <attribute name="authenticationIds" type="normalizedString" />
        <attribute name="responseSizeOctets" type="positiveInteger" />
        <attribute name="requestSizeOctets" type="positiveInteger" />
       </complexType>
     </element>
   </sequence>
  </complexType>
</element>

<element name="size">
  <complexType>
    <sequence>
      <element name="request" minOccurs="0" type="iristrans:octetsType" />
      <element name="response" minOccurs="0" type="iristrans:octetsType" />
    </sequence>
  </complexType>
</element>

<complexType name="octetsType">
  <choice>
    <element name="exceedsMaximum" />
    <element name="octets" type="positiveInteger" />
  </choice>
</complexType>

<element name="authenticationSuccess">
  <complexType>
    <sequence>
      <element name="description" minOccurs="0" maxOccurs="unbounded">
        <complexType>
          <simpleContent>
            <extension base="string">
              <attribute name="language" type="language" use="required"/>
            </extension>
          </simpleContent>
        </complexType>
      </element>
      <element name="data" minOccurs="0" maxOccurs="1" type="base64Binary"/>
    </sequence>
  </complexType>
</element>

<element name="authenticationFailure">
  <complexType>
    <sequence>
      <element name="description" minOccurs="0" maxOccurs="unbounded">
        <complexType>
          <simpleContent>
            <extension base="string">
              <attribute name="language" type="language" use="required"/>
            </extension>
          </simpleContent>
        </complexType>
      </element>
    </sequence>
  </complexType>
</element>
```

```
<element name="other">
 <complexType>
  <sequence>
   <element name="description" minOccurs="0" maxOccurs="unbounded">
    <complexType>
     <simpleContent>
      <extension base="string">
       <attribute name="language" type="language" use="required"/>
      </extension>
     </simpleContent>
    </complexType>
   </element>
  </sequence>
  <attribute type="token" name="type" use="required"/>
 </complexType>
</element>

</schema>
```

4. Informations de version

L'élément <versions> est utilisé pour décrire les informations de version du protocole de transfert, du protocole d'application et des modèles de données utilisés par le protocole d'application.

L'élément <versions> a un ou plusieurs éléments fils <transferProtocol>. Les éléments <transferProtocol> ont zéro, un ou plusieurs éléments fils <application>. Et les éléments <application> ont zéro, un ou plusieurs éléments <dataModel>. Chacun de ces types d'éléments a un attribut "protocolId" qui identifie le protocole qu'il représente et un attribut facultatif "extensionIds" qui identifie les extensions de protocole qu'il prend en charge.

Pendant la négociation des capacités, les deux parties de la négociation sont censées reconnaître la valeur "protocolId" de l'élément <transferProtocol> et au moins un des éléments <application> et <dataModel>. Si la négociation aboutit à une situation où cela n'est pas possible, une erreur DEVRAIT être signalée et la communication être interrompue. Il n'est pas prévu que chaque partie doive reconnaître les valeurs "extensionIds", et les valeurs "extensionIds" non reconnues DOIVENT être ignorées.

En outre, l'élément <transferProtocol> a des attributs facultatifs "authenticationIds", "responseSizeOctets" et "requestSizeOctets". L'attribut "authenticationIds" identifie les mécanismes d'authentification pris en charge par le protocole de transfert associé. L'attribut "responseSizeOctets" décrit la taille maximale de la réponse en octets que le serveur fournira. L'attribut 'requestSizeOctets' décrit la taille maximale de la demande en octets que le serveur acceptera.

Les identifiants de protocole, d'extension et de mécanisme d'authentification ne sont pas d'un type spécifique et le présent document n'en définit aucun. Les spécifications utilisant ce schéma XML DOIVENT définir les identifiants à utiliser avec l'élément <versions> et ses enfants.

La signification des octets pour le transfert de données est comptée de différentes manières selon les protocoles de transfert. Certains protocoles de transfert doivent seulement spécifier les octets des données transférées, tandis que d'autres protocoles de transfert doivent tenir compte des octets supplémentaires utilisés pour transférer les données. Les spécifications qui utilisent ce schéma XML DOIVENT décrire comment ces comptes d'octets sont calculés.

Voici un exemple de XML décrivant les informations de version.

```
<versions xmlns="urn:ietf:params:xml:ns:iris-transport">
 <transferProtocol protocolId="iris.lwz" authenticationIds="PLAIN EXTERNAL">
  <application protocolId="urn:ietf:params:xml:ns:iris1" extensionIds="http://example.com/SIMPLEBAG">
   <dataModel protocolId="urn:ietf:params:xml:ns:dchk1"/>
   <dataModel protocolId="urn:ietf:params:xml:ns:dreg1"/>
  </application>
 </transferProtocol>
```

```
</versions>
```

5. Informations de taille

L'élément <size> donne au serveur un moyen pour communiquer au client qu'une certaine demande a dépassé une taille négociée (<request>) ou qu'une réponse à une certaine demande va dépasser une taille négociée (<response>).

Un serveur peut indiquer une des deux conditions de taille en spécifiant les éléments fils suivants :

<exceedsMaximum> - cet élément fils indique simplement que la taille dépasse celle négociée.

<octets> - cet élément fils indique que la taille excède la taille négociée et il porte le nombre d'octets qui est le maximum pour une demande si l'élément parent est un élément <request> ou le nombre d'octets nécessaire à donner à la réponse si l'élément parent est un élément <response>.

La signification des octets pour le transfert de données est comptée de différentes manières selon les protocoles de transfert. Certains protocoles de transfert doivent seulement spécifier les octets des données transférées, tandis que d'autres protocoles de transfert doivent tenir compte des octets supplémentaires utilisés pour transférer les données. Les spécifications qui utilisent ce schéma XML DOIVENT décrire comment ces comptes d'octets sont calculés.

Voici un exemple de XML décrivant les informations de taille.

```
<size xmlns="urn:ietf:params:xml:ns:iris-transport">
  <response>
    <octets>1211</octets>
  </response>
</size>
```

6. Informations de succès d'authentification

L'élément <authenticationSuccess> indique qu'un client s'est authentifié avec succès auprès d'un serveur. Parallèlement à cette indication, il peut fournir un texte qui peut être présenté à un utilisateur concernant cette authentification réussie à l'aide d'éléments fils <description>.

Chaque élément <description> DOIT avoir un attribut "language" décrivant la langue du contenu de l'élément <description>. Les clients ne sont pas censés enchaîner plusieurs descriptions ; par conséquent, les serveurs NE DOIVENT PAS fournir plusieurs éléments <description> avec le même descripteur de langue.

Enfin, des données de sécurité supplémentaires peuvent être renvoyées avec le message de réussite de l'authentification en utilisant l'élément <data>. Le contenu de cet élément est du type simple base64Binary.

Voici un exemple de XML décrivant les informations de réussite d'authentification.

```
<authenticationSuccess
  xmlns="urn:ietf:params:xml:ns:iris-transport">
  <description language="fr">
    l'utilisateur 'bob' s'authentifie avec un mot de passe
  </description>
</authenticationSuccess>
```

Exemple de succès d'authentification

7. Informations d'échec d'authentification

L'élément <authenticationFailure> indique qu'un client a échoué à s'authentifier correctement auprès d'un serveur. Avec

cette indication, il peut fournir du texte qui peut être présenté à un utilisateur concernant cet échec d'authentification en utilisant des éléments fils <description>.

Chaque élément <description> DOIT avoir un attribut "language" qui décrit la langue du contenu de l'élément <description>. Les clients ne sont pas supposés enchaîner plusieurs descriptions ; donc, les serveurs NE DOIVENT PAS fournir plusieurs éléments <description> avec le même descripteur de langue.

Voici un exemple de XML décrivant des informations d'échec d'authentification.

```
<authenticationFailure
  xmlns="urn:ietf:params:xml:ns:iris-transport">
  <description language="fr">
    prière de consulter votre administrateur si vous avez oublié votre mot de passe
  </description>
</authenticationFailure>
```

Exemple d'échec d'authentification

8. Autres informations

L'élément <other> porte des informations d'état qui peuvent nécessiter une interprétation humaine pour être significatives. Cet élément possède un attribut "type" exigé, qui contient un identifiant de la nature des informations. Le présent document ne définit aucun identifiant à utiliser dans cet attribut, mais l'intention est que ces identifiants soient bien connus afin que les clients puissent effectuer différentes classes d'action en fonction du contenu de cet attribut. Par conséquent, les spécifications qui utilisent ce schéma XML DOIVENT définir ces identifiants.

L'élément <other> peut comporter zéro, un, ou plusieurs éléments <description>. Chaque élément <description> DOIT avoir un attribut "language" décrivant la langue du contenu de l'élément <description>. Les serveurs peuvent utiliser ces éléments fils pour porter des informations textuelles aux clients concernant la classe (ou le type) d'informations d'état spécifiées par l'élément <other>. Les clients ne sont pas censés enchaîner plusieurs descriptions ; par conséquent, les serveurs NE DOIVENT PAS fournir plusieurs éléments <description> avec le même descripteur de langue.

Voici un exemple de XML décrivant d'autres informations.

```
<other xmlns="urn:ietf:params:xml:ns:iris-transport" type="system">
  <description language="fr">
    indisponible, revenir plus tard
  </description>
</other>
```

Exemple d'autres informations

9. Considérations d'internationalisation

Les processeurs XML ont l'obligation de reconnaître les deux codages UTF-8 et UTF-16 [Unicode]. XML fournit les mécanismes pour identifier et utiliser d'autres codages de caractères. Les protocoles de transfert d'application DOIVENT définir quels sont les codages de caractères supplémentaires, si il en est, qui sont permis dans l'utilisation du XML défini dans le présent document.

10. Considérations relatives à l'IANA

Le présent document utilise le registre d'espace de noms et de schéma XML spécifié dans XML_URN [RFC3688]. En conséquence, les enregistrements suivants ont été faits par l'IANA :

o URN d'espace de noms XML : urn:ietf:params:xml:ns:iris-transport

Contact : Andrew Newton <andy@hxr.us>
XML : aucun

o URN de schéma XML : urn:ietf:params:xml:schema:iris-transport
Contact : Andrew Newton <andy@hxr.us>
XML : le schéma XML spécifié à la Section 3

11. Considérations sur la sécurité

Les protocoles de transfert qui utilisent XML conformément au schéma XML du présent document et qui offrent des propriétés de sécurité comme l'authentification et la confidentialité DEVRAIENT offrir un message initial du serveur au client utilisant l'élément <versions>. Cet élément <versions> DEVRAIT contenir tous les identifiants d'authentification pertinents dans son attribut "authenticationId". L'objet de la fourniture de ce message initial est d'aider à déjouer les attaques en dégradation.

12. Références

12.1 Références normatives

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

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

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3", ISBN 0-201-61633-5, 2000.

[XML] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0", W3C XML, février 1998, <http://www.w3.org/TR/1998/REC-xml-19980210>.

[XML-Esp] World Wide Web Consortium, "Namespaces in XML", W3C XML Namespaces, janvier 1999, <http://www.w3.org/TR/1999/REC-xml-names-19990114>.

[XML-Data] World Wide Web Consortium, "XML Schema Part 2: Datatypes", W3C XML Schema, octobre 2004, <http://www.w3.org/TR/xmlschema-2/>.

[XML-Str] World Wide Web Consortium, "XML Schema Part 1: Structures", W3C XML Schema, octobre 2004, <http://www.w3.org/TR/xmlschema-1/>.

12.2 Références pour information

[RFC3981] A. Newton, M. Sanz, "IRIS : Protocole central du service d'information des registres Internet (IRIS)", janvier 2005. (*MàJ par* RFC4992) *(P.S.)*

[RFC4992] A. Newton, "Traitement XML en parallèle avec tronçons pour le service d'information de registre Internet", août 2007. (*MàJ* RFC3981 ; *P.S. ; MàJ par* RFC8996)

[RFC4993] A. Newton, "Protocole léger de transfert UDP pour le service d'information de registre Internet", août 2007. *(P.S.)*

Appendice A. Contributeurs

Des contributions substantielles au présent document ont été fournies par les membres du groupe de travail CRISP de l'IETF, en particulier Robert Martin-Legene, Milena Caires, et David Blacka.

Adresse de l'auteur

Andrew L. Newton
VeriSign, Inc.
21345 Ridgetop Circle
Sterling, VA 20166
USA

téléphone : +1 703 948 3382
mél : andy@hxr.us
URI : http://www.verisignlabs.com/

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.