Groupe de travail Réseau
Request for Comments : 5361
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

G. Camarillo, Ericsson

octobre 2008

Format de document pour demander le consentement

Résumé
Le présent document définit un format de langage de balisage extensible (XML, *Extensible Markup Language*) pour un document de permission utilisé pour demander le consentement. Un document de permission écrit dans ce format est utilisé par un relais pour demander la permission à un receveur spécifique d'effectuer une traduction d'acheminement particulière.

Table des matières

1. Introduction

Le cadre pour les communications fondées sur le consentement dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC5360] identifie le besoin d'un format pour créer des documents de permission. Ces documents de permission sont utilisés par les relais SIP [RFC3261] pour demander la permission d'effectuer des traductions. Un relais est défini comme tout serveur SIP, qu'il soit mandataire, agent d'utilisateur de bout en bout (B2BUA, *Back-to-Back User Agent*) ou un mélange des deux, qui reçoit une demande et traduit l'URI de demande en un ou plusieurs URI de prochain bond auxquels il livre alors une demande.

Le format des documents de permission spécifié dans le présent document se fonde sur la politique commune [RFC4745], un format de document XML pour exprimer les préférences de confidentialité.

2. Définitions et terminologie

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].

Le présent document utilise les termes définis dans la [RFC5360]. Pour être complet, ces termes sont répétés ici. La Figure 1 de la [RFC5360] montre les relations entre les URI de cible et les URI de receveur dans une opération de traduction.

URI de receveur : URI de demande d'une demande sortante envoyée par une entité (par exemple, un agent d'utilisateur ou un mandataire). L'envoi d'une telle demande peut avoir été le résultat d'une opération de traduction.

Relais : tout serveur SIP, qu'il soit un mandataire, un agent d'utilisateur de bout en bout (B2BUA, *Back-to-Back User Agent*) ou un mélange des deux, qui reçoit une demande, traduit son URI de demande en un ou plusieurs URI de prochain bond (c'est-à-dire, des URI de receveur) et livre la demande à ces URI.

URI cible : URI de demande d'une demande entrante arrivant à un relais qui va effectuer une opération de traduction.

Logique de traduction : logique qui définit une opération de traduction à un relais. Cette logique inclut les URI cible et receveur de la traduction.

Opération de traduction : opération par laquelle un relais traduit l'URI de demande d'une demande entrante (c'est-à-dire, l'URI cible) en un ou plusieurs URI (c'est-à-dire, des URI de receveur) qui sont utilisés comme URI de demande d'une ou plusieurs demandes sortantes.

3. Structure du document de permission

Un document de permission est un document XML, formaté conformément au schéma défini dans la [RFC4745]. Les documents de permission héritent du type MIME des documents de politique commune, "application/auth-policy+xml". Comme décrit dans la [RFC4745], ce type de document est composé de trois parties : conditions, actions, et transformations.

Cette section définit les nouvelles conditions et actions définies par la présente spécification. Cette spécification ne définit aucune nouvelle transformation.

3.1 Conditions

Les conditions dans un document de permission sont un ensemble d'expressions, dont chacune s'évalue à VRAI ou FAUX. Noter que, comme discuté dans la [RFC4745], un document de permission s'applique à une traduction si toutes les expressions dans sa partie conditions s'évaluent à VRAI.

3.1.1 Condition de receveur

La condition de receveur est confrontée à l'URI de receveur d'une traduction. Les conditions de receveur peuvent contenir les mêmes éléments et attributs comme conditions d'identité.

Quand il effectue une traduction, un relais confronte la condition de receveur du document de permission qui a été utilisé pour demander la permission pour cette traduction à l'URI de destination de la demande sortante. Quand il reçoit une demande accordant ou refusant des permissions (par exemple, une demande SIP PUBLISH comme décrit dans la [RFC5360]) le relais confronte la condition de receveur du document de permission qui a été utilisé pour demander la permission à l'identité de l'entité qui accorde ou refuse les permissions (c'est-à-dire, l'envoyeur de la demande PUBLISH). Si il y a concordance, la condition de receveur s'évalue à VRAI. Autrement, la condition de receveur s'évalue à FAUX.

Comme seules des entités authentifiées peuvent être confrontées, ce paragraphe définit les moyens acceptables d'authentification, qui sont en ligne avec ceux décrits au paragraphe 5.6.1 de la [RFC5360]. L'attribut "id" dans les éléments <one> et <except> DOIVENT contenir un schéma quand ces éléments apparaissent dans un document de

permission.

Quand il est utilisé avec SIP, un receveur qui accorde ou refuse des permissions au relais est considéré être authentifié si une des techniques suivantes est utilisée :

Identité SIP [RFC4474], comme décrit au paragraphe 5.6.1.1 de la [RFC5360]. Pour les demandes PUBLISH qui sont authentifiées en utilisant le mécanisme Identité SIP, l'identité de l'envoyeur de la demande PUBLISH est égale à l'URI SIP du champ d'en-tête From de la demande, en supposant que la signature dans le champ d'en-tête Identité a été validée.

P-Asserted-Identity [RFC3325] (qui ne peut être utilisée que dans des environnements de réseau clos) comme décrit au paragraphe 5.6.1.2 de la [RFC5360]. Pour les demandes PUBLISH qui sont authentifiées en utilisant le mécanisme P-Asserted-Identity, l'identité de l'envoyeur de la demande PUBLISH est égale au champ d'en-tête P-Asserted-Identity de la demande.

Essai d'acheminement de retour, comme décrit au paragraphe 5.6.1.3 de la [RFC5360]. Il peut être utilisé pour les demandes SIP PUBLISH et HTTP GET. Aucune authentification n'est supposée être utilisée avec l'essai d'acheminement de retour et donc, aucune procédure de confrontation d'identité n'est définie.

Résumé SIP, comme décrit au paragraphe 5.6.1.4 de la [RFC5360]. L'identité de l'envoyeur est réglée égale à l'adresse d'enregistrement (AOR, *Address of Record*) SIP pour l'utilisateur qui s'est authentifié lui-même.

3.1.2 Condition d'identité

La condition d'identité, qui est définie dans la [RFC4745], est confrontée à l'URI de l'envoyeur de la demande qui est utilisée comme entrée pour une traduction.

Quand il effectue une traduction, un relais confronte la condition d'identité à l'identité de l'envoyeur de la demande entrante. Si elles correspondent, la condition d'identité s'évalue à VRAI. Autrement, la condition d'identité s'évalue à FAUX.

Comme seules des entités authentifiées peuvent être confrontées, les paragraphes qui suivent définissent les moyens acceptables d'authentification, la procédure pour représenter l'identité de l'envoyeur comme un URI, et la procédure pour convertir un identifiant de la forme utilisateur@domaine, présent dans l'attribut "id" des éléments <one> et <except>, en un URI.

3.1.2.1 Moyens d'authentification acceptables

Quand elle est utilisée avec SIP, une demande envoyée par un envoyeur est considérée authentifiée si une des techniques suivantes est utilisée :

Résumé SIP : le relais authentifie l'envoyeur en utilisant l'authentification par résumé SIP [RFC2617]. Cependant, si l'authentification anonyme décrite au paragraphe 22.1 de la [RFC3261] est utilisée, l'envoyeur n'est pas considéré comme authentifié.

Identité affirmée : si une demande contient un champ d'en-tête P-Asserted-ID [RFC3325] et si la demande vient d'un élément de confiance, l'envoyeur est considéré comme authentifié.

Identité vérifiée cryptographiquement : si une demande contient un champ d'en-tête Identité comme défini dans la [RFC4474], et qu'elle valide le champ d'en-tête From de la demande, la demande est considérée être authentifiée. Noter que ceci est vrai même si la demande contenait un champ d'en-tête From de la forme sip:anonymous@exemple.com. Tant que la signature vérifie que la demande vient légitimemet de cette identité, elle est considérée être authentifiée.

3.1.2.2 Calcul d'un URI pour l'envoyeur

Pour les demandes qui sont authentifiées en utilisant le résumé SIP, l'identité de l'envoyeur est réglée égale à l'adresse d'enregistrement SIP pour l'utilisateur qui s'est authentifié lui-même. Par exemple, considérons l'enregistrement d'utilisateur suivant dans une base de données :

SIP AOR: sip:alice@exemple.com

digest username: ali
digest password: f779ajvvh8a6s6
digest realm: exemple.com

Si le relais reçoit une demande et la met au défi avec son domaine réglé à "exemple.com", et que la demande suivante contient un champ d'en-tête Autorisation avec un nom d'utilisateur de "ali" et une réponse de résumé générée avec le mot de passe "f779ajvvh8a6s6", l'identité utilisée dans les opérations de confrontation est "sip:alice@exemple.com".

Pour les demandes qui sont authentifiées en utilisant la [RFC3325], l'identité de l'envoyeur est égale à l'URI SIP dans le champ d'en-tête P-Asserted-ID. Si il y a plusieurs valeurs pour le champ d'en-tête P-Asserted-ID (il peut y avoir un URI sip et un URI tel [RFC3966]) alors chacun d'eux est utilisé pour les comparaisons mentionnées dans la [RFC4745] ; si l'une d'elles correspond à un élément <one> ou <except>, elle est considérée correspondre.

Pour les demandes qui sont authentifiées en utilisant le mécanisme d'identité SIP [RFC4474], l'identité de l'envoyeur est égale à l'URI SIP dans le champ d'en-tête From de la demande, en supposant que la signature dans le champ d'en-tête Identité a été validé.

SIP permet aussi les demandes anonymes. Si une une demande est anonyme parce que le défi/réponse de résumé utilisait le nom d'utilisateur "anonymous", la demande est considérée comme non authentifiée et ne va pas correspondre à la condition <identity>. Si une demande est anonyme parce que elle contient un champ d'en-tête Privacy [RFC3323], mais contient quand même un champ d'en-tête P-Asserted-ID, l'identité dans le champ d'en-tête P-Asserted-ID est utilisée dans les calculs d'autorisation ; le fait que la demande soit anonyme n'a pas d'impact sur le traitement de l'identité. Cependant, si la demande a traversé une frontière de confiance et si le champ d'en-tête P-Asserted-ID et le champ d'en-tête Privacy ont été supprimés, la demande va être considérée comme non authentifiée quand elle arrive au relais, et donc ne satisfait pas la condition <sender>. Finalement, si une demande contenait un champ d'en-tête Identité qui était validé, et si le champ d'en-tête From contenait un URI de la forme sip:anonymous@exemple.com, alors l'envoyeur est considéré comme authentifié, et il va avoir un identité égale à sip:anonymous@exemple.com. Si une telle identité avait été placée dans un élément <one> ou <except>, il y aurait une correspondance.

3.1.2.3 Calcul d'un URI SIP à partir de l'attribut d'identifiant

Si la condition <one> ou <except> ne contient pas de schéma, la conversion de la valeur de l'attribut "id" en un URI SIP est triviale. Si les caractères dans l'attribut "id" sont des caractères valides pour les composants utilisateur et partie hôte de l'URI SIP, un "sip:" est ajouté au contenu de l'attribut "id", et le résultat est L'URI SIP. Si les caractères dans l'attribut "id" ne sont pas valides pour les composants utilisateur et partie hôte de l'URI SIP, la conversion n'est pas possible et donc, la condition d'identité s'évalue à FAUX. Cela arrive, par exemple, quand la portion utilisateur de l'attribut "id" contient des caractères UTF-8.

3.1.3 Condition de cible

La condition de cible est confrontée à l'URI de cible d'une traduction. La condition de cible peut contenir les mêmes éléments et attributs que les conditions d'identité.

Quand il effectue une traduction, un relais confronte la condition de cible à la destination de la demande entrante, qui est normalement contenue dans l'URI de demande. Si elles correspondent, la condition de cible s'évalue à VRAI. Autrement, la condition de cible s'évalue à FAUX.

3.1.4 Condition de validité

L'élément <validity> n'est pas applicable à ce document. Chaque élément <permission> a une durée de vie infinie et peut être révoqué en utilisant un mécanisme indépendant, comme décrit au paragraphe 5.8 de la [RFC5360]. Dans tous les cas, comme expliqué au paragraphe 4.1 de la [RFC5360], les permissions ne sont valides qu'autant que le contexte où elles ont été accordées est valide. Si il en est de présents, les éléments <validity> DOIVENT être ignorés.

3.1.5 Condition de sphère

L'élément <sphere> n'est pas applicable à ce document et n'est donc pas utilisé. Si il en est de présents, les éléments <sphere> DOIVENT être ignorés.

3.2 Actions

Les actions dans un document de permission fournissent des URI pour accorder ou refuser la permission d'effectuer la traduction décrite dans le document.

Noter que l'élément <trans-handling> n'est pas une action, comme défini dans la politique commune [RFC4745], mais plutôt un élément d'information. Donc, le mécanisme de résolution de conflit ne s'applique pas à lui.

Chaque règle de politique contient au moins deux éléments <trans-handling> ; un élément avec un URI pour accorder, et un autre avec un URI pour refuser, la permission.

3.2.1 Traitement de traduction

Le <trans-handling> fournit des URI pour qu'un receveur accorde ou refuse au relais la permission d'effectuer une traduction. Les valeurs définies sont :

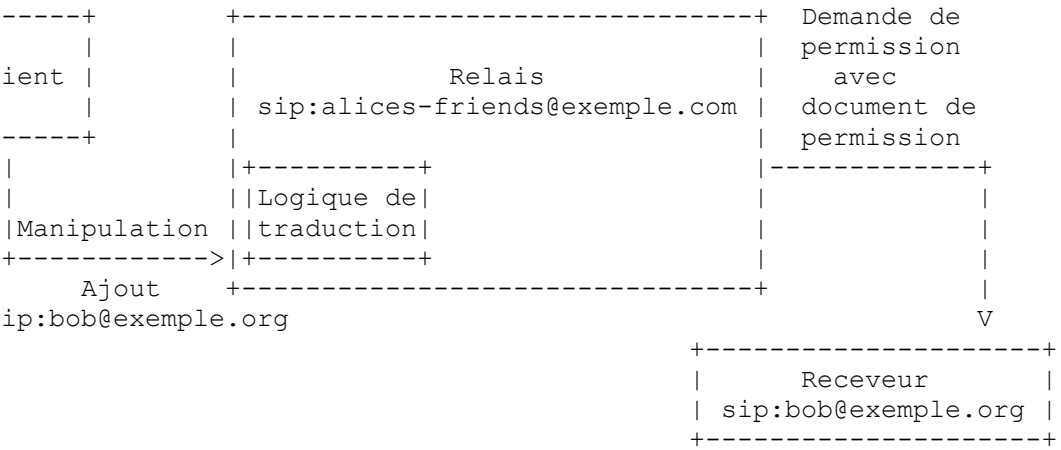
deny : cette action dit au relais de ne pas effectuer la traduction.

grant : cette action dit au serveur d'effectuer la traduction.

L'attribut "perm-uri" dans l'élément <trans-handling> fournit un URI pour accorder ou refuser la permission d'effectuer une traduction.

4. Exemple de document

Dans l'exemple suivant, un client ajoute "sip:bob@exemple.org" à la traduction dont l'URI de cible est "sip:alices-friends@exemple.com". Le relais qui traite la traduction génère le document de permission suivant afin de demander la permission de relayer les demandes envoyées à "sip:alices-friends@exemple.com" à "sip:bob@exemple.org". L'URI de cible est "sip:alices-friends@exemple.com", et l'URI de receveur est "sip:bob@exemple.org". L'identité de l'envoyeur ne joue pas de rôle dans cet exemple. Donc, le document de permission ne met aucune restriction sur les envoyeurs potentiels.




```
<?xml version="1.0" encoding="UTF-8"?>
   <cp:ruleset
     xmlns="urn:ietf:params:xml:ns:consent-rules"
     xmlns:cp="urn:ietf:params:xml:ns:common-policy">
     <cp:rule id="f1">
    <cp:conditions>
      <cp:identity>
        <cp:many/>
      </cp:identity>
      <recipient>
```

```
            <cp:one id="sip:bob@exemple.org"/>
          </recipient>
          <target>
            <cp:one id="sip:alices-friends@exemple.com"/>
          </target>
        </cp:conditions>
        <cp:actions>
          <trans-handling
            perm-uri="sips:grant-1awdch5Fasddfce34@exemple.com"
            >grant</trans-handling>
          <trans-handling
            perm-uri="https://exemple.com/grant-1awdch5Fasddfce34"
            >grant</trans-handling>
          <trans-handling
            perm-uri="sips:deny-23rCsdfgvdT5sdfgye@exemple.com"
            >deny</trans-handling>
          <trans-handling
            perm-uri="https://exemple.com/deny-23rCsdfgvdT5sdfgye"
            >deny</trans-handling>
        </cp:actions>
        <cp:transformations/>
      </cp:rule>
      </cp:ruleset>
```

5. Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>
  <xs:schema
    targetNamespace="urn:ietf:params:xml:ns:consent-rules"
    xmlns:cr="urn:ietf:params:xml:ns:consent-rules"
    xmlns:cp="urn:ietf:params:xml:ns:common-policy"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

<!-- Conditions -->
    <xs:element name="recipient" type="cp:identityType"/>
    <xs:element name="target" type="cp:identityType"/>

<!-- Actions -->
   <xs:simpleType name="trans-values">
     <xs:restriction base="xs:string">
       <xs:enumeration value="deny"/>
       <xs:enumeration value="grant"/>
     </xs:restriction>
    </xs:simpleType>

    <xs:element name="trans-handling">
     <xs:complexType>
       <xs:simpleContent>
         <xs:extension base="trans-values">
           <xs:attribute name="perm-uri" type="xs:anyURI" use="required"/>
         </xs:extension>
       </xs:simpleContent>
     </xs:complexType>
    </xs:element>

  </xs:schema>
```

6. Extensibilité

La présente spécification définit des éléments qui n'ont pas de points d'extension dans l'espace de noms "urn:ietf:params:xml:ns:consent-rules". Les documents d'instances qui utilisent ces définitions d'éléments DEVRAIENT être des schémas valides. Les applications qui traitent les documents d'instance avec un contenu qui n'est pas compris par l'application DOIVENT ignorer ce contenu. Les documents d'extension de l'IETF de cette spécification PEUVENT réutiliser l'espace de noms "urn:ietf:params:xml:ns:consent-rules" pour définir de nouveaux éléments.

7. Considérations relatives à l'IANA

Cette Section enregistre un nouvel espace de noms XML et un nouveau schéma XML selon les procédures de la [RFC3688].

7.1 Enregistrement d'espace de noms XML

URI : urn:ietf:params:xml:ns:consent-rules

Contact d'enregistrement : groupe de travail SIPPING de l'IETF à <sipping@ietf.org>,
Gonzalo Camarillo <Gonzalo.Camarillo@ericsson.com>

XML :

DÉBUT

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
       content="text/html;charset=iso-8859-1"/>
  <title>Espace de noms des règles de consentement</title>
</head>
<body>
  <h1>Espace de noms pour les documents de permission</h1>
  <h2>urn:ietf:params:xml:ns:consent-rules</h2>
<p>See <a href="http://www.rfc-editor.org/rfc/rfc5361.txt">RFC 5361
  </a>.</p>
</body>
</html>
```

FIN

7.2 Enregistrement de schéma XML

URI : urn:ietf:params:xml:schema:consent-rules

Contact d'enregistrement : groupe de travail SIPPING de l'IETF à <sipping@ietf.org>,
Gonzalo Camarillo <Gonzalo.Camarillo@ericsson.com>

XML : Le schéma XML à enregistrer est contenu dans la Section 5.

8. Considérations sur la sécurité

La [RFC5360] discute les problèmes relatifs à la sécurité, comme comment authentifier les demandes SIP et HTTP qui demandent des permissions et comment transporter les documents de permission entre les relais et les receveurs, qui sont en relation directe avec la présente spécification.

9. Remerciements

Jonathan Rosenberg a fourni des idées utiles sur ce document. Hannes Tschofenig a aidé à aligner ce document sur la politique courante. Ben Campbell et Mary Barnes ont effectué une relecture serrée de ce document. Lakshminath Dondeti a fourni d'utiles commentaires.

10. Références

10.1 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)

[RFC2617] J. Franks et autres, "Authentification HTTP : Authentification d'accès de base et par résumé", juin 1999. *(DS.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3323] J. Peterson, "Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)", novembre 2002.

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

[RFC4474] J. Peterson et C. Jennings, "Améliorations de la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", août 2006. *(P.S. ; Remplacée par* RFC8224)

[RFC4475] R. Sparks et autres, "Messages d'essais de résistance du protocole d'initialisation de session (SIP)", mai 2006. *(Info.)*

[RFC5360] J. Rosenberg et autres, "Cadre des communications fondées sur le consentement dans le protocole d'initialisation de session (SIP)", octobre 2008. *(P.S. ; MàJ par* RFC8217)

10.2 Références pour information

[RFC3325] C. Jennings, J. Peterson et M. Watson, "Extensions privées au protocole d'initialisation de session (SIP) pour l'assertion d'identité au sein de réseaux de confiance", novembre 2002. *(Information ; MàJ par* RFC8217)

[RFC3966] H. Schulzrinne, "L'URI tel pour les numéros de téléphone", décembre 2004. (*MàJ par* RFC5341) *(P.S.)*

Adresse de l'auteur

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland
mél : Gonzalo.Camarillo@ericsson.com

Déclaration complète de droits de reproduction