Groupe de travail Réseau
Request for Comments : 4827
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

M. Isomaki
E. Leppanen
Nokia

mai 2007

Utilisation du protocole d'accès de configuration (XCAP) du langage de balisage extensible (XML) pour la manipulation des contenus de documents Presence

Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document décrit une utilisation du protocole d'accès de configuration du langage de balisage extensible (XML, *Extensible Markup Language*) (XCAP, *XML Configuration Access Protocol*) pour la manipulation du contenu des documents de présence fondés sur le format de données d'informations de présence (PIDF, *Presence Information Data Format*). Il est destiné à être utilisé dans les systèmes de présence fondés sur le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) où le composeur d'état d'événement peut utiliser le document de présence manipulé par XCAP comme une des entrées sur lesquelles il va construire l'état de présence global pour la présentité.

Table des Matières

1. Introduction

La spécification du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) pour la messagerie instantanée et la présence (SIMPLE, *SIP Instant Messaging and Presence*) permet à un utilisateur, appelé un observateur *(watcher)*, de s'abonner à un autre utilisateur, appelé une présentité, afin d'apprendre ses informations de présence [7]. Le modèle des données de présence a été spécifié dans [10]. Le modèle des données fait une séparation nette entre informations de personne, de service, et d'appareil.

Un mécanisme fondé sur SIP, la méthode SIP PUBLISH, a été défini pour la publication de l'état de présence [4]. En utilisant la méthode PUBLISH de SIP, un agent d'utilisateur de présence (PUA, *Presence User Agent*) peut publier sa vue de l'état de présence, indépendamment de et sans qu'il soit besoin d'acquérir la connaissance des états constitués par d'autres PUA. Cependant, la méthode PUBLISH de SIP a une portée limitée et ne satisfait pas à toutes les exigences d'établissement d'un état de présence. Le principal problème est que PUBLISH crée un état conditionnel qui arrive à expiration après la fin

de la durée de vie négociée sauf si il est rafraîchi. Cela la rend inutilisable pour les cas où l'état devrait perdurer sans qu'il y ait d'appareil actif capable de rafraîchir l'état.

Il y a trois principaux cas d'utilisation dans lesquels est utile l'établissement d'un état de présence permanent indépendant de l'activité de tout appareil particulier. Le premier cas concerne l'établissement d'un état en relation avec la personne. La présentité voudrait souvent établir son état de présence même lors de périodes dans lesquelles il n'y a pas d'appareil actif disponible capable de publication. Les bons exemples sont les voyages, vacances, et ainsi de suite. Le second cas est à propos de l'établissement d'état pour des services qui sont ouverts à la communication, même si la présentité n'a pas un appareil qui fasse fonctionner ce service en ligne. Des exemples de cette sorte de services incluent la messagerie électronique, le service de messagerie multimédia (MMS, *Multimedia Messaging Service*), et le service de messages courts (SMS, *Short Message Service*). Dans ces services, la présentité est fournie avec un serveur qui rend le service disponible en permanence, au moins sous certaines formes, et il serait bon d'être capable de l'annoncer aux observateurs. Comme il n'est pas réaliste de supposer que tous les serveurs de messagerie électronique, de MMS, ou de SMS puissent publier d'eux-mêmes l'état de présence (et même si c'était possible, un tel état ne changerait presque jamais), cela doit être fait par un autre appareil. Et comme la disponibilité du service ne dépend pas de cet appareil, il serait impraticable d'exiger de cet appareil qu'il soit constamment actif juste pour publier une telle disponibilité. Le troisième cas concerne l'établissement de l'état par défaut de toute personne, service, ou appareil en l'absence de tout appareil capable de publier activement un tel état. Par exemple, la présentité peut vouloir annoncer que son service vocal est actuellement fermé, juste pour faire savoir aux observateurs qu'un tel service pourrait être ouvert à certains moments. Là encore, ce type d'état par défaut est indépendant de tout appareil particulier et peut être considéré comme assez persistent.

Bien que la méthode PUBLISH de SIP reste la voie principale d'annonce de l'état de présence dans les systèmes de présence fondés sur SIMPLE et soit particulièrement bien adaptée pour la publication d'états dynamiques (ce qu'est principalement la présence) elle a besoin d'être complétée par le mécanisme décrit dans le présent document pour traiter les cas d'utilisation présentés ci-dessus.

Le protocole d'accès à une configuration XML (XCAP, *XML Configuration Access Protocol*) [2] permet à un client de lire, écrire, et modifier des données de configuration d'application mémorisées en format XML sur un serveur. Les données n'ont pas de délai d'expiration, aussi doivent elles être explicitement insérées et supprimées. Le protocole permet que plusieurs clients manipulent les données, pourvu qu'ils y soient autorisés. XCAP est déjà utilisé dans les systèmes de présence fondés sur SIMPLE pour la manipulation des listes de présence et des politiques d'autorisation de présence. Cela fait de XCAP un choix idéal pour faire de la manipulation de document de présence indépendante de l'appareil.

Le présent document définit l'utilisation d'application du protocole d'accès de configuration XML (XCAP) pour la manipulation des contenus de document de présence. Le format de document d'information de présence (PIDF, *Presence Information Document Format*) [3] est utilisé comme format de document de présence, car le composeur d'état d'événement doit déjà le prendre en charge du fait qu'il est utilisé dans la méthode PUBLISH de SIP.

La Section 3 décrit en détail comment le document de présence manipulé par XCAP se rapporte à la publication d'état conditionnel effectuée avec la méthode PUBLISH de SIP.

XCAP exige des utilisations d'application qu'elles normalisent plusieurs éléments d'information, y compris un identifiant d'application (AUID, *Application Usage ID*) unique et un schéma XML pour les données manipulées. Ceci est spécifié à partir de la Section 4.

2. Conventions

Dans le présent document, les mos clés 'DOIT', 'NE DOIT PAS', 'EXIGE, 'DEVRA', 'NE DEVRA PAS', 'DEVRAIT', 'NE DEVRAIT PAS', 'RECOMMANDE', 'PEUT', et 'FACULTATIF' sont à interpréter comme décrit dans la RFC 2119 [1] et indiquent des niveaux d'exigence pour les mises en œuvre conformes.

Une terminologie complète de présence et des états d'événement publiés est fournie dans "Extension au protocole d'initialisation de session (SIP) pour la publication d'état d'événement" [4].

3. Relations avec l'état de présence publié en utilisant SIP PUBLISH

Le cadre de publication de l'état de présence est décrit à la Figure 1. Une partie centrale du cadre est l'élément de composeur d'état d'événement, dont la fonction est de composer les informations de présence reçues de plusieurs sources en un seul document cohérent de présence.

L'état de présence manipulé avec XCAP peut être vu comme une des sources d'informations pour le composeur à combiner avec les informations d'état mou publiées en utilisant SIP PUBLISH. Ceci est illustré à la Figure 1. On s'attend à ce que, dans le cas normal, il puisse y avoir plusieurs PUA qui publient leurs vues séparées avec SIP PUBLISH, mais seulement un unique document de présence manipulé avec XCAP. Comme le montre la figure, plusieurs clients XCAP (par exemple, dans des appareils physiques différents) peuvent manipuler le même document sur le serveur XCAP, mais cela ne crée qu'une seule entrée pour le composeur d'état d'événement. Le serveur XCAP mémorise le document de présence manipulé par XCAP sous l'arborescence "utilisateurs" dans la hiérarchie des documents XCAP. Voir les détails à la Section 9 et un exemple à la Section 11.

Comme entrées individuelles, les états de présence établis par XCAP et par SIP PUBLISH sont complètement séparés, et il n'est pas possible de manipuler directement les états établis par un mécanisme avec l'autre. La façon dont le composeur traite les entrées fondées sur XCAP par rapport aux entrées fondées sur SIP PUBLISH est l'affaire des politiques de composeur, qui sortent du domaine d'application de la présente spécification. Comme la spécification SIP PUBLISH rend déjà obligatoire que le composeur soit capable de construire l'état de présence global à partir de plusieurs entrées, qui peuvent contenir des informations non orthogonales (ou d'une certaine façon même conflictuelles) cette utilisation de XCAP n'impose aucune nouvelle exigence à la fonction de composeur.

Figure 1 : Cadre de la publication de présence et de la composition d'état d'événement

L'interface de protocole entre le serveur XCAP et le composeur d'état d'événement n'est pas spécifiée ici.

4. Identifiant d'usage d'application

XCAP exige que l'utilisation d'application définisse un identifiant d'utilisation d'application unique (AUID) aussi bien dans l'arborescence IETF que dans une arborescence de fabricant. La présente spécification définit l'AUID 'pidf-manipulation' au sein de l'arborescence IETF, via l'enregistrement par l'IANA à la Section 13.

5. Type MIME

Le type MIME pour cette utilisation d'application est 'application/pidf+xml'.

6. Structure des informations de présence manipulées

Le schéma XML des informations de présence est défini dans le format de données des informations de présence (PIDF, *Presence Information Data Format*) [3]. Le PIDF définit aussi un mécanisme d'extension des informations de présence. Voir dans [8], [9], [11], et [12] les extensions de PIDF actuellement définies et leurs schémas XML.

L'URI d'espace de nom pour PIDF est 'urn:ietf:params:xml:ns:pidf' qui est aussi l'espace de nom de document XCAP par défaut.

7. Contraintes supplémentaires

Il n'y a pas d'autres contraintes sur le document que celles décrites dans les schémas XML (PIDF et ses extensions) et dans la description de PIDF [3].

8. Interdépendance des ressources

Il n'y a pas d'interdépendance des ressources au delà de la possible interdépendance définie dans PIDF [3] et XCAP [2] qui doive être définie pour cette utilisation d'application.

9. Conventions de dénomination

Le serveur XCAP DOIT mémoriser un seul document de présence manipulé par XCAP pour chaque utilisateur. Le document de présence DOIT être localisé sous l'arborescence "utilisateurs", en utilisant le nom de fichier "index". Voir un exemple à la Section 11.

10. Politiques d'autorisation

La présente utilisation d'application ne modifie pas la politique d'autorisation de XCAP par défaut, qui permet seulement à un utilisateur (propriétaire) de lire, écrire ou modifier ses propres documents. Un serveur peut permettre à des utilisateurs privilégiés de modifier des documents dont ils ne sont pas propriétaires, mais l'établissement et l'indication de telles politiques est en-dehors du domaine d'application du présent document.

11. Exemple

Cette section donne un exemple d'un document de présence fourni par un client XCAP à un serveur XCAP. Le document de présence illustre la situation dans laquelle une présentité (humain) est partie en vacances, et avant cela, a établi ses informations de présence de telle sorte qu'il ne soit disponible que via la messagerie électronique. En l'absence de toute information d'état mou publiée, ce serait la seule entrée au composeur qui forme le document de présence. Le document qui sert d'exemple contient les extensions PIDF spécifiées dans "RPID : Extensions Rich Presence au format de données d'information Presence (PIDF)" [8] et dans "CIPID : Informations de contact pour le format de données d'information Presence" [9].

On supposera que la présentité est un utilisateur SIP avec une adresse d'enregistrement (AOR, *Address-of-Record*) sip:someone@example.com. L'URI racine XCAP pour example.com est supposée être http://xcap.example.com. L'identifiant d'utilisateur (XUI, *User Identifier*) XCAP est supposé être identique à l'AOR SIP, conformément aux recommandations XCAP. Dans ce cas, le document de présence serait situé à http://xcap.example.com/pidf-manipulation/users/ sip:someone@example.com/index.

Le document de présence est créé avec l'opération XCAP suivante :

PUT /pidf-manipulation/users/sip:someone@example.com/index HTTP/1.1Host: xcap.example.com
Content-Type: application/pidf+xml
...

```
<?xml version="1.0" encoding="UTF-8"?>
      <presence xmlns="urn:ietf:params:xml:ns:pidf"
          xmlns:rp="urn:ietf:params:xml:ns:pidf:rpid"
          xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
          xmlns:ci="urn:ietf:params:xml:ns:pidf:cipid"
          entity="sip:someone@example.com">
     <tuple id="x8eg92m">
        <status>
        <basic>closed</basic>
        </status>
        <rp:user-input>idle</rp:user-input>
        <rp:class>auth-1</rp:class>
        <contact priority="0.5">sip:user@example.com</contact>
        <note>Je ne suis joignable que par mél.</note>
        <timestamp>2004-02-06T16:49:29Z</timestamp>
      </tuple>
       <tuple id="x8eg92n">
        <status>
          <basic>open</basic>
        </status>
        <rp:class>auth-1</rp:class>
        <contact priority="1.0">mailto:someone@example.com</contact>
        <note>Je lis mes mél deux fois par semaine</note>
       </tuple>
```

```
  <dm:person id="p1">
    <rp:class>auth-A</rp:class>
    <ci:homepage>http://www.example.com/~someone</ci:homepage>
    <rp:activities>
       <rp:vacation/>
    </rp:activities>
  </dm:person>
</presence>
```

Lorsque l'utilisateur veut changer la note qui se rapporte au service de messagerie électronique, il le fait avec l'opération XCAP suivante :

```
PUT /pidf-manipulation/users/sip:someone@example.com/index/
~~/presence/tuple%5b@id='x8eg92n'%5d/note HTTP/1.1
If-Match: "xyz"
ost: xcap.example.com
Content-Type: application/xcap-el+xml
...

<note>Je lis mes mél les mardis et vendredis</note>
```

12. Considérations pour la sécurité

Un document présence contient des informations qui sont très sensibles. Sa livraison aux observateurs doit absolument se faire en se conformant strictement aux politiques d'autorisation pertinentes. Il est aussi important que seuls les clients autorisés soient capables de manipuler les informations de présence.

La spécification de base de XCAP rend obligatoire que tous les serveurs XCAP mettent en œuvre l'authentification par résumé HTTP spécifiée dans la RFC 2617 [5]. De plus, les serveurs XCAP DOIVENT mettre en œuvre HTTP sur TLS [6]. Il est recommandé que les administrateurs de serveurs XCAP utilisent un URI HTTPS comme URI de service racine XCAP, de façon que le résumé d'authentification de client se fasse sur TLS. En utilisant ces moyens, le client et le serveur XCAP peuvent assurer la confidentialité et l'intégrité des opérations de manipulation de document de présence XCAP, et que seuls les clients autorisés ont la possibilité de le faire.

13. Considérations relatives à l'IANA

Il y a des considérations relatives à l'IANA associées à la présente spécification.

13.1 Identifiant d'utilisation d'application XCAP

Ce paragraphe enregistre un nouvel identifiant d'utilisation d'application XCAP (AUID, *Application Usage ID*) conformément aux procédures de l'IANA définies dans [2].

Nom de l'AUID : pidf-manipulation

Description : l'utilisation d'application Pidf-manipulation définit comment XCAP est utilisé pour manipuler le contenu des documents de présence fondés sur PIDF.

14. Remerciements

Les auteurs tiennent à remercier Jari Urpalainen, Jonathan Rosenberg, Hisham Khartabil, Aki Niemi, Mikko Lonnfors, Oliver Biot, Alex Audu, Krisztian Kiss, Jose Costa-Requena, George Foti et Paul Kyzivat de leurs commentaires.

15. Références

15.1 Références normatives

[1] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", RFC2119, BCP 14, mars 1997.

[2] J. Rosenberg, "Protocole d'accès de configuration (XCAP) du langage de balisage extensible (XML)", RFC4825, mai 2007.

[3] H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, W. Carr et J. Peterson, "Format des données d'information de présence (PIDF)", RFC3863, août 2004.

[4] A. Niemi, "Extension au protocole d'initialisation de session (SIP) pour la publication d'état d'événement", RFC3903, octobre 2004.

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

[6] E. Rescorla, "HTTP sur TLS", RFC 2818, mai 2000. *(Information)*

15.2 Références pour information

[7] J. Rosenberg, "Paquetage d'événement Presence pour le protocole d'initialisation de session (SIP)", RFC3856, août 2004.

[8] H. Schulzrinne, V. Gurbani, P. Kyzivat et J. Rosenberg, "RPID : Extensions Rich Presence au format de données d'information Presence (PIDF)", RFC4480, juillet 2006.

[9] H. Schulzrinne, "CIPID : Informations de contact pour le format de données d'information Presence", RFC4482, juillet 2006.

[10] J. Rosenberg, "Modèle de données pour Presence", RFC4479, juillet 2006. *(P.S.)*

[11] M. Lonnfors, K. Kiss, "Extension de capacité d'agent d'utilisateur au format de données d'information de présence (PIDF) du protocole d'initialisation de session (SIP)", RFC5196, septembre 2008. *(P.S.)*

[12] H. Schulzrinne, "Extensions Présence synchronisée au format de données d'information Presence (PIDF) pour indiquer les informations d'état pour les intervalles de temps passés et futurs", RFC4481, juillet 2006. *(P.S.)*

Adresse des auteurs

Markus Isomaki
Nokia
P.O. BOX 100
00045 NOKIA GROUP
Finland
mél : markus.isomaki@nokia.com

Eva Leppanen
Nokia
P.O. BOX 785
33101 Tampere
Finland
mél : eva-maria.leppanen@nokia.com

Déclaration complète de droits de reproduction

COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF