Groupe de travail Réseau
Request for Comments : 2935
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

D. Eastlake, Motorola
C. Smith, Royal Bank of Canada
septembre 2000

Supplément HTTP au protocole Internet de commerce ouvert (IOTP)

Résumé
Les messages du protocole de commerce ouvert sur l'Internet (IOTP, *Internet Open Trading Protocol*) vont être portés comme des documents de langage de balisage extensible (XML, *Extensible Markup Language*). À ce titre, le but de la transposition en la couche de transport est de s'assurer que les documents XML sous-jacents sont portés avec succès entre les diverses parties.

Le présent document décrit cette transposition pour le protocole de transport hypertexte (HTTP, *Hyper Text Transport Protocol*) versions 1.0 et 1.1.

Table des matières

1. Introduction

Les messages du protocole de commerce ouvert sur l'Internet (IOTP, *Internet Open Trading Protocol*) [RFC2801] vont être portés comme des documents [XML]. À ce titre, le but de la transposition en la couche de transport est de s'assurer que les documents XML sous-jacents sont portés avec succès entre les diverses parties.

Le présent document décrit cette transposition pour le protocole de transport hypertexte (HTTP, *Hyper Text Transport Protocol*) versions 1.0 [RFC1945] et 1.1 [RFC2616].

De futurs documents pourront décrire IOTP sur messagerie électronique (SMTP), TCP, TV par câble, ou autres transports.

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. Serveurs et clients HTTP

La structure de IOTP se transpose en la structure de HTTP de la façon suivante :

Les rôles de commerçant, de traitement de payement, de traitement de livraison, et de soin de consommateur sont tous représentés par des serveurs HTTP. Chacun peut être représenté par un serveur séparé, ou ils peuvent être combinés de toutes les façons.

Le rôle de consommateur est représenté par un client HTTP.

Note : un commerçant, peut agir dans le rôle de consommateur, par exemple pour déposer un payement électronique. Dans ce cas, le commerçant, comme organisation plutôt que comme rôle, va devoir être pris en charge par un client HTTP.

3. Localisations Net HTTP

Les localisations Net contenues dans la spécification IOTP sont toutes des URI [RFC 2396]. Si une connexion sûre est requise ou désirée, un canal sûr que prennent tous deux en charge le serveur et le client HTTP DOIT être utilisée. Des exemples de tels canaux sont SSL version 3 ou TLS [RFC 2246].

4. Clients de consommateur

Dans la plupart des environnements, l'agent de consommateur va initialement être un navigateur HTML. Cependant, les navigateurs courants ne fournissent pas la capacité nécessaire pour agir comme un agent pour le consommateur pour une transaction IOTP. Cela conduit à deux exigences :
- une méthode pour lancer et passer le contrôle au client IOTP,
- et une méthode pour fermer proprement le client IOTP et repasser le contrôle au navigateur HTML une fois que la transaction IOTP est finie.

4.1 Lancement du client IOTP et du serveur de commerçant IOTP

À un certain point, le client HTTP chez le consommateur va envoyer une demande HTTP qui est interprétée comme une "demande de commencer IOTP" par le serveur du commerçant HTTP. Cela pourrait, par exemple, être le résultat d'un clic sur un bouton "payer". Ce message tient lieu d'un message de demande d'une certaine forme et le serveur de commerçant va répondre par le premier message IOTP sous la forme d'un document XML.

Le type MIME pour tous les messages IOTP est : "APPLICATION/IOTP" ; cependant "APPLICATION/X-IOTP" a été utilisé pour l'expérimentation et le développement et DEVRAIT aussi être reconnu. Voir à la Section 7 ci-dessous le gabarit d'enregistrement de type MIME pour APPLICATION/IOTP. Parce que HTTP est purement binaire, aucun codage de transfert de contenu n'est requis. (Voir dans la [RFC2376] le type application/xml qui a des considérations assez similaires.)

Cette réponse HTTP va être interprétée par le navigateur HTML comme une demande de commencer l'application associée au type MIME "APPLICATION/IOTP", et de passer le contenu de ce message à cette application.

À ce point, le client IOTP va être lancé et avoir le premier message.

Les messages IOTP ont une courte durée de vie. Donc, le serveur HTTP DEVRAIT éviter de mettre ses réponses en antémémoire. Dans HTTP v1.0, le paramètre "nocache" peut être utilisé. Ceci peut être négligé sur des connexions sécurisées par SSL/TLS qui ne sont pas mises en antémémoire et sur les demandes HTTP POST dans HTTP v1.1 car dans v1.1 les réponses POST ne sont pas mises en antémémoire.

4.2 Messages IOTP sortants

Les données provenant des messages IOTP antérieurs dans une transaction DOIVENT être conservées par le client IOTP afin qu'elles puissent (1) être copiées pour faire partie des messages IOTP ultérieurs, (2) utilisées dans les calculs de

vérification des signatures dans les message IOTP ultérieurs, (3) être renvoyées dans certains cas où une demande est arrivée en fin de temporisation sans réponse, (4) utilisées comme entrée au rôle de soin de consommateur dans les dernières versions de IOTP, etc. La façon dont les données sont copiées dépend de la transaction IOTP. Les données DOIVENT être conservées jusqu'à la fin de la transaction, que ce soit un succès, un échec, ou une annulation, et tant que ensuite il est désiré pour qu'une des parties enquête sur elles.

Les messages IOTP contiennent des localisations Net (par exemple, PayReqNetLocn) qui pour HTTP vont contenir les URI auxquels le client IOTP DOIT envoyer les messages IOTP.

Les messages IOTP suivants (des documents XML) vont être envoyés en utilisant les fonctions POST de HTTP. Le client HTTP DOIT effectuer des demandes HTTP POST complètes.

Les documents XML DOIVENT être envoyés d'une manière compatible avec les codages externes permis par la spécification [XML].

4.3 Arrêt d'une transaction IOTP

Ce qui suit devrait être lu en conjonction avec la [RFC 2801].

Une transaction IOTP est achevée quand :

- le client IOTP décide de faire échouer la transaction IOTP pour une raison quelconque soit en annulant la transaction, soit par suite de la découverte d'une erreur dans un message IOTP reçu, ou

- une "fin de temporisation" se produit ou une connexion échoue, par exemple, une réponse à un message IOTP n'a pas été reçue après une certaine période définie par l'utilisateur (incluant des retransmissions).

Un client IOTP qui traite une transaction IOTP qui :

- s'achève avec succès (c'est-à-dire, elle n'a pas reçu un bloc Erreur avec une HardError ou un bloc Cancel) DOIT diriger le navigateur sur la localisation Net spécifiée dans SuccessNetLocn dans le composant Options de protocole, c'est-à-dire, l'amener à faire un HTTP GET avec cet URL ;

- ne s'achève pas par un succès, parce qu'il a reçu un bloc "Error Trading", DOIT afficher les informations du message d'erreur, arrêter la transaction, et passer le contrôle au navigateur afin qu'il fasse un GET sur la "Error Net Location" spécifiée pour le rôle d'où l'erreur a été reçue ;

- est annulée parce qu'un bloc Cancel a été reçu, DOIT arrêter la transaction IOTP et passer le contrôle au navigateur afin qu'il fasse un GET sur la "Cancel Net Location" spécifiée pour le rôle d'où le bloc Cancel a été reçu ;

- est erronée parce que un message IOTP ne se conforme pas à cette spécification, DOIT envoyer un message IOTP contenant un bloc "Error Trading" au rôle d'où le message erroné a été reçu et le ErrorLogNetLoc spécifié pour ce rôle, arrêter la transaction IOTP, et passer le contrôle au navigateur afin qu'il fasse un GET à partir de la "Error Net Location" spécifiée pour le rôle d'où le mauvais message a été reçu ;

- a une "fin de temporisation", DOIT afficher un message décrivant la fin de temporisation, PEUT donner à l'utilisateur l'option d'annuler ou de réessayer et/ou peut automatiquement réessayer. Sur un échec dû à une fin de temporisation, traiter comme une erreur ci-dessus.

Chaque mise en œuvre d'un client IOTP peut décider de terminer ou non l'application de client IOTP immédiatement à l'achèvement d'une transaction IOTP ou d'attendre qu'elle soit close par suite, par exemple, de la clôture de l'utilisateur ou du navigateur.

5. Lancement des serveurs de traitement de payement et de livreur IOTP

Les serveurs de traitement de payement et de livraison sont lancés par la réception d'un message IOTP qui contient :
- pour un traitement de payement, un bloc de demande de payement,
- pour un traitement de livraison, un bloc de demande de livraison.

6. Considérations de sécurité

La sécurité des messages du protocole de commerce ouvert sur l'Internet est principalement assurée par les signatures dans IOTP décrites dans les [RFC 2801] et [RFC 2802]. La protection de la confidentialité pour les interactions IOTP peut être obtenue en utilisant un canal sûr pour les messages IOTP, tel que SSL/TLS [RFC2246].

Noter que la sécurité des protocoles de payement transportés par IOTP est le la responsabilité de ces protocoles de payement, et NON de IOTP.

7. Considérations relatives à l'IANA

La présente spécification définit le type MIME APPLICATION/IOTP. Le gabarit d'enregistrement suit la spécification de la [RFC 2048] :

To: ietf-types@iana.org
Subject : enregistrement du type de support MIME APPLICATION/IOTP
Nom du type de support MIME : APPLICATION
Nom du sous type MIME : IOTP
Paramètres exigés : (aucun)
Paramètres facultatifs : charset – voir la RFC 2376
Considérations de codage : le contenu est XML et peut dans certains cas exiger un codage "quoted printable" ou "base64". Cependant, aucun codage n'est requis pour le transport HTTP qui est prévu être courant.
Considérations de sécurité : IOTP inclut des dispositions pour l'authentification numérique, mais pour la confidentialité, d'autres mécanismes comme TLS devraient être utilisés. Voir la RFC 2801 et la RFC 2802.
Considérations d'interopérabilité : voir la RFC 2801.
Spécification publiée : voir les RFC 2801 et RFC 2802.
Applications qui utilisent ce type de support : applications du protocole de commerce ouvert sur l'Internet.
Informations supplémentaires : (aucune)
Adresse de messagerie de la personne à contacter pour plus d'informations :
nom : Donald E. Eastlake 3rd
mél : Donald.Eastlake@motorola.com
Usage prévu : COMMUN
Auteur/Contrôleur des changements : IETF

8. Références

[RFC1945] T. Berners-Lee, R. Fielding, H. Frystyk, "Protocole de transfert Hypertext -- HTTP/1.0", mai 1996. *(Information)*

[RFC2048] N. Freed, J. Klensin et J. Postel, "Extensions multi-objets de la messagerie Internet (MIME) Partie 4 : Procédures d'enregistrement", BCP 13, novembre 1996. *(Rendue obsolète par les RFC* 4288-4289)

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[RFC2376] E. Whitehead et M. Murata, "Types de support XML", juillet 1998.

[RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir* RFC3986)

[RFC2616] R. Fielding et autres, "Protocole de transfert hypertexte -- HTTP/1.1", juin 1999. *(D.S., MàJ par* 2817, 6585)

[RFC2801] D. Burdett, "Protocole Internet du commerce ouvert - IOTP version 1.0", avril 2000. *(Information)*

[RFC2802] K. Davidson, Y. Kawatsura, "Signatures numériques pour la v1.0 du protocole Internet du commerce ouvert (IOTP)", avril 2000. *(Information)*

[XML] Bray, T., Paoli, J. and C. Sperberg-McQueen, "Extensible Markup Language (XML) 1.0", févier 1998.

9. Adresse des auteurs

Donald E. Eastlake 3rd
Motorola
140 Forest Avenue
Hudson, MA 01749
USA
téléphone : +1 508-261-5434(w)
Fax : +1 508-261-4447(w)
mél : Donald.Eastlake@motorola.com

Chris J. Smith
Royal Bank of Canada
277 Front Street West
Toronto, Ontario M5V 3A4
CANADA
téléphone : +1 416-348-6090
Fax: +1 416-348-2210
mél : chris.smith@royalbank.com

10. Déclaration complète de droits de reproduction

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