Groupe de travail Réseau
Request for Comments : 5734
STD : 69
RFC rendue obsolète : 4934
Catégorie : Norme

S. Hollenbeck, VeriSign, Inc.
août 2009

Traduction Claude Brière de L'Isle

Transport sur TCP du protocole d'approvisionnement extensible (EPP)

Résumé
Le présent document décrit comment une session de protocole d'approvisionnement extensible (EPP, *Extensible Provisioning Protocol*) est transposée sur une seule connexion de protocole de contrôle de transmission (TCP, *Transmission Control Protocol*). Cette transposition exige l'utilisation du protocole de sécurité de la couche Transport (TLS, *Transport Layer Security*) pour protéger les informations échangées entre un client EPP et un serveur EPP. Le présent document rend obsolète la RFC 4934.

Table des Matières

1. Introduction

Le présent document décrit comment le protocole d'approvisionnement extensible (EPP, *Extensible Provisioning Protocol*) se transpose sur une seule connexion client-serveur TCP. Les services de sécurité au delà de ceux définis dans EPP sont fournis par le protocole de sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC2246]. EPP est décrit dans la [RFC5730]. TCP est décrit dans la [RFC0793]. Le présent document rend obsolète la [RFC4934].

1.1 Conventions de notation utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Gestion de session

La transposition des facilités de gestion de session EPP sur le service TCP est directe. Une session EPP exige la création d'une connexion TCP entre deux homologues, un qui initie la demande de connexion et un qui répond à la demande de connexion. L'homologue initiateur est appelé le "client", et l'homologue qui répond est appelé le "serveur". Un serveur EPP DOIT écouter les demandes de connexion TCP sur un accès TCP standard alloué par l'IANA.

Le client DOIT produire un appel OPEN actif, spécifiant le numéro d'accès TCP sur lequel le serveur écoute les tentatives de connexion EPP. Le serveur EPP DOIT retourner un <greeting> EPP au client après l'établissement de la session TCP.

Une session EPP est normalement terminée par le client qui produit une commande EPP <logout>. Un serveur qui reçoit une commande EPP <logout> DOIT terminer la session EPP et clore la connexion TCP avec un appel CLOSE. Un client PEUT terminer une session EPP en produisant un appel CLOSE.

Un serveur PEUT limiter la durée de vie d'une connexion TCP établie. Les sessions EPP qui sont inactives pendant une durée définie par le serveur PEUVENT être closes par la production par le serveur d'un appel CLOSE. Un serveur PEUT aussi clore les connexions TCP qui ont été ouvertes et actives pour plus longtemps que la période définie par le serveur.

3. Échanges de messages

À l'exception de l'accueil du serveur EPP, les messages EPP sont initiés par le client EPP sous la forme de commandes EPP. Un serveur EPP DOIT retourner une réponse EPP à une commande EPP sur la même connexion TCP qui a porté la commande. Si la connexion TCP est close après qu'un serveur a reçu et traité avec succès une commande mais avant que la réponse puisse être retournée par le client, le serveur PEUT tenter de supprimer les effets de la commande pour assurer un état cohérent entre le client et le serveur. Les commandes EPP sont idempotentes, de sorte que traiter une commande plus d'une fois produit le même effet net sur le répertoire que le traitement réussi une seule fois de la commande.

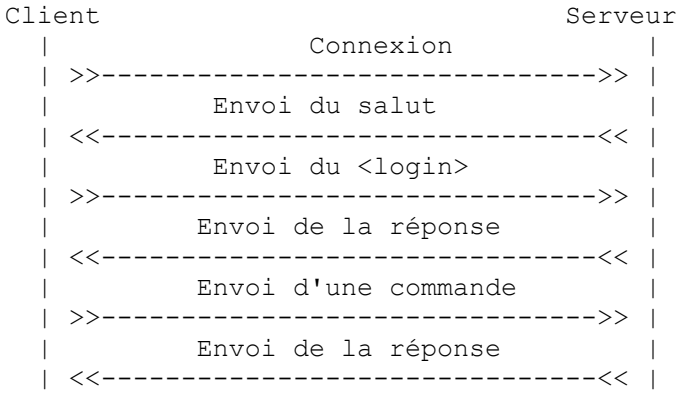
Un client EPP envoie les commandes EPP à un serveur EPP sur une connexion TCP établie. Un client NE DOIT PAS distribuer les commandes à partir d'une seule session EPP sur plusieurs connexions TCP. Un client PEUT établir plusieurs connexions TCP pour prendre en charge plusieurs sessions EPP dont chacune se transpose sur une seule connexion. Un serveur DEVRAIT limiter un client à un nombre maximum de connexions TCP sur la base des capacités du serveur et de la charge de fonctionnement.

EPP décrit les interactions client-serveur comme un échange de commande-réponse dans lequel le client envoie une commande au serveur et le serveur retourne une réponse au client. Un client peut être capable de réaliser un petit gain de performances en traitant en parallèle les commandes (en envoyant plus d'une commande avant qu'une réponse à la première commande soit reçue) avec le transport TCP, mais cette caractéristique ne change pas le mode de fonctionnement à une seule commande, une seule réponse du cœur de protocole.

Chaque unité de données EPP DOIT contenir un seul message EPP. Les commandes DOIVENT être traitées de façon indépendante et dans le même ordre que celui de l'envoi du client.

Un serveur DEVRAIT imposer une limite au temps requis par un client pour produire une commande EPP bien formée. Un serveur DEVRAIT mettre fin à une session EPP et clore une connexion TCP ouverte si une commande bien formée n'est pas reçue dans cette limite.

Un automate à états général pour un serveur EPP est décrit à la Section 2 de la [RFC5730]. L'échange général de messages client-serveur utilisant le transport TCP est illustré à la Figure 1.



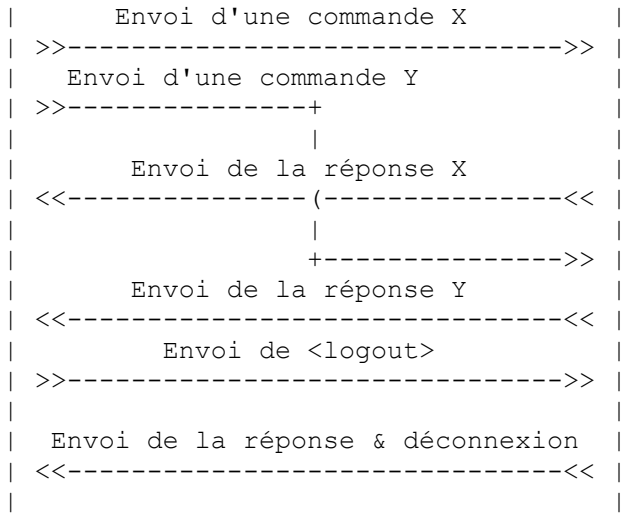
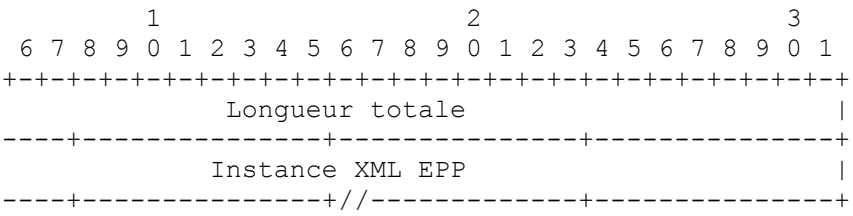


Figure 1 : Échange TCP de messages client-serveur

4. Format d'unité de données

L'unité de données EPP contient deux champs : un en-tête de 32 bits qui décrit la longueur totale de l'unité de données, et l'instance XML EPP. La longueur de l'instance XML EPP est déterminée en soustrayant quatre octets de la longueur totale de l'unité de données. Un receveur doit réussir à lire ce nombre d'octets pour restituer l'instance XML EPP complète avant de traiter le message EPP.

Format d'unité de données EPP (un cran représente une position de bit) :



Longueur totale (32 bits) : La longueur totale de l'unité de données EPP mesurée en octets dans l'ordre des octets du réseau (gros boutien). Les octets contenus dans ce champ DOIVENT être inclus dans le calcul de la longueur totale.

Instance XML EPP (longueur variable) : C'est l'instance XML EPP portée dans l'unité de données.

5. Considérations de transport

Le paragraphe 2.1 de la spécification cœur du protocole EPP [RFC5730] décrit les considérations sur les transpositions du transport du protocole. Le présent document traite chacune de ces considérations en utilisant une combinaison de caractéristiques décrites dans le document et de caractéristiques fournies par TCP comme suit :

- TCP comporte des dispositifs pour assurer la fiabilité, le contrôle de flux, l'ordre de livraison, et le contrôle de l'encombrement. Le paragraphe 1.5 de la [RFC0793] décrit ces dispositifs en détail ; les principes du contrôle de l'encombrement sont aussi décrits dans la [RFC2581] et la [RFC2914]. TCP est un protocole en mode connexion, et la Section 2 du présent document décrit comment les sessions EPP sont transposées sur les connexions TCP.
- Les Sections 2 et 3 du présent document décrivent comment la nature à états pleins de EPP est préservée à travers les sessions gérées et les échanges contrôlés de messages.
- La Section 3 du présent document note que le traitement en parallèle de commandes est possible avec TCP, bien que le traitement par lots (combinant plusieurs commandes EPP dans une seule unité de données) ne soit pas permis.
- La Section 4 du présent document décrit les dispositifs pour tramer les unités de données en spécifiant explicitement le nombre d'octets utilisés pour représenter une unité de données.

6. Considérations d'internationalisation

Le présent document n'introduit ni ne présente aucune question d'internationalisation ou de localisation.

7. Considérations relatives à l'IANA

Le numéro d'accès de système 700 a été alloué par l'IANA pour la transposition de EPP sur TCP.

Le numéro d'accès d'utilisateur 3121 (qui était utilisé pour des besoins de développement et d'essais) a été repris par l'IANA.

8. Considérations pour la sécurité

EPP tel qu'il est assure simplement des service d'authentification de client en utilisant des identifiants et des mots de passe en clair. Une attaque passive est suffisante pour récupérer les identifiants et mots de passe de client ce qui permet une falsification triviale des commandes. La protection contre la plupart des autres attaques courantes DOIT être fournie par d'autres couches de protocole.
Lorsque elle est mise en couche sur TCP, la version 1.0 du protocole de sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC2246] ou ses successeurs (comme TLS 1.2 [RFC5246]), en utilisant la plus récente version prise en charge par les deux parties, DOIT être utilisée pour assurer l'intégrité, la confidentialité, et une authentification mutuelle forte du client et du serveur. Les mises en œuvre de TLS contiennent souvent un mode cryptographique faible qui NE DEVRAIT PAS être utilisé pour protéger EPP. Les clients et serveurs qui désirent une forte sécurité DEVRAIENT plutôt utiliser TLS avec des algorithmes de chiffrement qui sont moins susceptibles de compromission.

L'authentification qui utilise le protocole de prise de contact TLS confirme l'identité des machines de client et de serveur. EPP utilise un identifiant et un mot de passe de client supplémentaires pour identifier et authentifier l'identité d'utilisateur du client auprès du serveur, complétant l'authentification des machines fournie par TLS. L'identité décrite dans le certificat de client et l'identité décrite dans l'identifiant de client EPP peuvent différer, car un serveur peut allouer plusieurs identités d'utilisateur pour l'usage d'une machine de client particulière. Les identités de certificat acceptables DOIVENT être négociées entre les opérateurs de client et les opérateurs de serveur en utilisant un mécanisme hors bande. Les identités de certificat présentées DOIVENT correspondre aux identités négociées avant que le service EPP soit accepté.

Il y a un risque de compromission des accréditifs de connexion si un client n'identifie pas correctement un serveur avant de tenter d'établir une session EPP. Avant d'envoyer des accréditifs de connexion au serveur, un client doit confirmer que le certificat de serveur reçu dans la prise de contact TLS est un certificat attendu pour le serveur. Un client doit aussi confirmer que le salut reçu du serveur contient les informations d'identification attendues. Après l'établissement d'une session TLS et la réception d'un salut EPP sur une connexion TCP protégée, les clients DOIVENT comparer le sujet du certificat et/ou le subjectAltName aux informations d'identification de serveur attendues et interrompre le traitement si une discordance est détectée. Si la validation de certificat réussit, le client doit alors s'assurer que les informations contenues dans le certificat el le salut reçus sont cohérents et appropriés. Comme décrit ci-dessus, les deux vérifications exigent normalement un échange hors bande d'informations entre le client et le serveur pour identifier les valeurs attendues avant de tenter des connexions dans la bande.

Les serveurs TCP EPP sont vulnérables aux attaques de déni de service courantes sur TCP incluant l'inondation de SYN TCP. Les serveurs DEVRAIENT prendre des mesures pour minimiser l'impact d'une attaque de déni de service en utilisant des combinaisons de solutions faciles à mettre en œuvre, comme le déploiement de la technologie du pare-feu et des filtres de routeur bordure pour restreindre l'accès entrant au serveur à des clients connus et de confiance.

9. Profil d'usage TLS

Le client devrait initier une connexion avec le serveur et envoyer ensuite le Hello de client TLS pour commencer la prise de contact TLS. Lorsque la prise de contact TLS est terminée, le client peut alors envoyer le premier message EPP.

Il est EXIGÉ des mises en œuvre de TLS qu'elles prennent en charge la suite de chiffrement obligatoire spécifiée dans la version mise en œuvre :
- TLS 1.0 [RFC2246] : TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS 1.1 [RFC4346] : TLS_RSA_WITH_3DES_EDE_CBC_SHA

- TLS 1.2 [RFC5246] : TLS_RSA_WITH_AES_128_CBC_SHA

Le présent document est supposé s'appliquer aux futures versions de TLS, auquel cas la suite de chiffrement obligatoire pour la version mise en œuvre DOIT être prise en charge.

L'authentification mutuelle du client et du serveur en utilisant le protocole de prise de contact TLS est EXIGÉE. Les signatures sur le chemin complet de certification pour les deux machines de client et de serveur DOIVENT être validées au titre de la prise de contact TLS. Les informations incluses dans le certificat de client et de serveur, comme les périodes de validité et les noms des machines, DOIVENT aussi être validées. Une description complète des problèmes associés à la validation du chemin de certification se trouve dans la [RFC5280]. Le service EPP NE DOIT PAS être accordé tant que ne sont pas achevées avec succès la prise de contact TLS et la validation de certificat, assurant que les deux machines du client et du serveur ont été authentifiées et que les protections cryptographiques sont en place.

Si le client a des informations externes sur l'identité que doit présenter le serveur, la vérification du nom du serveur PEUT être omise. Par exemple, un client peut se connecter à une machine dont l'adresse et le nom de serveur sont dynamiques, mais dont le client connaît le certificat que va présenter le serveur. Dans de tels cas, il est important de rétrécir la portée des certificats acceptables autant que possible afin de prévenir les attaques par interposition. Dans des cas particuliers, il peut être approprié que le client ignore simplement l'identité du serveur, mais on doit comprendre que cela laisse la connexion ouverte à une attaque active.

Durant la négociation TLS, le client EPP DOIT vérifier sa compréhension du nom et de l'adresse IP du serveur par rapport à l'identité de serveur telle que présentée dans le message Certificate du serveur afin de prévenir une attaque par interposition. Dans cette section, la compréhension du client de l'identité du serveur est appelée "identité de référence". La vérification est effectuée selon les règles suivantes dans l'ordre spécifié :

- Si l'identité de référence est un nom de serveur :
  - Si une extension subjectAltName du type dNSName [X.509] est présente dans le certificat du serveur, elle DEVRAIT alors être utilisée comme source de l'identité du serveur. La confrontation est effectuée comme décrit au paragraphe 7.2 de la [RFC5280], avec l'exception que la correspondance de caractères génériques (voir ci-dessous) est permise pour le type dNSName. Si le certificat contient plusieurs noms (par exemple, plus d'un champ dNSName) une correspondance avec l'un des champs est considérée comme acceptable.
  - Le caractère générique '*' (ASCII 42) est permis dans les valeurs de subjectAltName du type dNSName, et seulement comme étiquette de gauche (celle de poids fort) du DNS dans cette valeur. Ce caractère générique correspond à toute étiquette DNS de gauche dans le nom de serveur. C'est à dire que le sujet *.example.com correspond aux noms de serveur a.example.com et b.example.com, mais ne correspond pas pour example.com ou a.b.example.com.
  - L'identité du serveur PEUT aussi être vérifiée en comparant l'identité de référence à la valeur du nom commun (CN, *Common Name*) [RFC4519] dans la branche Nom distinctif relatif (RDN, *Relative Distinguished Name*) du champ subjectName du certificat du serveur. Cette comparaison est effectuée en utilisant les règles de comparaison des noms du DNS des deux premiers points ci-dessus (y compris la correspondance de caractère générique). Bien que l'utilisation de la valeur du CN soit de pratique courante, elle est déconseillée, et les autorités de certification sont invitées à fournir à la place des valeurs de subjectAltName. Noter que la mise en œuvre de TLS peut représenter les DN dans les certificats conformément à X.500 ou à d'autres conventions. Par exemple, certaines mises en œuvre de X.500 rangent les RDN dans un DN en utilisant une convention de gauche à droite (du plus fort poids au moindre poids) au lieu de la convention de LDAP de droite à gauche.
- Si l'identité de référence est une adresse IP :
  - Le subjectAltName iPAddress DEVRAIT être utilisé par le client pour la comparaison. Dans un tel cas, l'identité de référence DOIT être convertie en représentation de chaîne d'octet "dans l'ordre des octets du réseau". Pour IPv4 (comme spécifié dans la [RFC0791]), la chaîne d'octets va contenir exactement quatre octets. Pour IPv6 (spécifié dans la [RFC2460]) la chaîne d'octets va contenir exactement seize octets. Cette chaîne d'octets est alors comparée aux valeurs de subjectAltName de type iPAddress. Une correspondance se produit si la chaîne d'octets de l'identité de référence et les chaînes d'octet de valeur sont identiques.

Si la vérification d'identité du serveur échoue, les clients en mode utilisateur DEVRAIENT soit le notifier à l'utilisateur (les clients PEUVENT dans ce cas donner à l'utilisateur l'opportunité de continuer la session EPP) soit clore la connexion de transport et indiquer que l'identité du serveur est suspecte. Les clients automatisés DEVRAIENT retourner ou enregistrer une erreur indiquant que l'identité du serveur est suspecte et/ou DEVRAIENT clore la connexion de transport. Les clients automatisés PEUVENT fournir un réglage de configuration qui désactive cette vérification, mais DOIVENT fournir un réglage qui l'active.

Durant la négociation TLS, le serveur EPP DOIT vérifier que le certificat du client correspond à l'identité de référence négociée précédemment hors bande, comme spécifié à la Section 8. Le serveur devrait satisfaire au nom de sujet ou au subjectAltName entiers comme décrit dans la RFC 5280. Le serveur PEUT appliquer d'autres restrictions au subjectAltName, par exemple si il sait qu'un certain client se connecte toujours à partir d'un certain nom d'hôte ou adresse IP.

Tous les messages EPP DOIVENT être envoyés comme "données d'application" TLS. Il est possible que plusieurs messages EPP soient contenus dans un enregistrement TLS, ou qu'un message EPP soit transféré dans plusieurs enregistrements TLS.

Lorsque aucune donnée n'est reçue pendant longtemps sur une connexion (c'est l'application décide de ce que "long" signifie) un serveur PEUT clore la connexion. Le serveur DOIT tenter d'initier un échange d'alertes close_notify avec le client avant de clore la connexion. Les serveurs qui ne sont pas prêts à recevoir d'autres données PEUVENT clore la connexion après l'envoi de l'alerte close_notify, générant ainsi une clôture incomplète du côté client.

10. Remerciements

La RFC 3734 a été produite par le groupe de travail PROVREG, qui a suggéré des améliorations et fourni de nombreux commentaires précieux. L'auteur souhaite remercier de leurs efforts les présidents du groupe de travail Edward Lewis et Jaap Akkerhuis pour leurs contributions au traitement et à la rédaction. La RFC 4934 et le présent document sont des soumissions individuelles, fondées sur le travail effectué dans la RFC 3734.

Des suggestions spécifiques incorporées dans le présent document ont été fournies par Chris Bason, Randy Bush, Patrik Faltstrom, Ned Freed, James Gould, Dan Manley, et John Immordino.

11. Références

11.1 Références normatives

[X.509] Recommandation UIT-T X.509, "Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire : Cadre d'authentification". Union Internationale des Télécommunications, Genève, novembre 1988.

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par* 5095, 6564 *; D.S)*

[RFC4519] A. Sciberras, éd., "Protocole léger d'accès à un répertoire (LDAP) : Schéma pour les applications d'utilisateur", juin 2006.

[RFC5730] S. Hollenbeck, "Protocole d'approvisionnement extensible (EPP)", STD0069, août 2009. *(Remplace la RFC4930)*

11.2 Références pour information

[RFC2580] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Déclarations de conformité pour SMIv2", avril 1999. (STD0058)

[RFC2914] S. Floyd, "Principes du contrôle d'encombrement", BCP 41, septembre 2000.

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, RFC4680, RFC4681, RFC5746, RFC6176, RFC7465, RFC7507, RFC7919)

[RFC4934] S. Hollenbeck, "Transport sur TCP avec le protocole d'approvisionnement extensible (EPP)", mai 2007. (*Remplace la* RFC3734) *(Remplacée par* RFC5734, STD 69)

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", août 2008. (*Remplace* RFC3268, RFC4346, RFC4366) (*MàJ* RFC4492) (*MàJ par* RFC5746, RFC5878)*(P.S.)*

[RFC5280] D. Cooper et autres, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", mai 2008. (*Remplace les* RFC3280, RFC4325, RFC4630) *(P.S.)*

Appendice A. Changements depuis la RFC 4933

1. On a changé "Le présent document rend obsolète la RFC3734" en "Le présent document rend obsolète la RFC4934".

2 On a remplace la référence à la RFC3280 par la référence à la RFC5280.

3. On a remplace la référence à la RFC3734 par la référence à la RFC4934.

4. On a mis à jour la référence à la RFC4346 et à TLS 1.1 par la référence à la RFC5246 et TLS 1.2.

5. On a remplace la référence à la RFC4930 par la référence à la RFC5730.

6. On a ajouté un paragraphe pour préciser le profil d'usage de TLS et inclus des références.

7. On a déplacé le paragraphe qui commence par "L'authentification mutuelle du client et du serveur" de la section des considérations sur la sécurité à la section Profil d'usage de TLS.

Adresse de l'auteur

Scott Hollenbeck
VeriSign, Inc.
21345 Ridgetop Circle
Dulles, VA 20166-6503
USA
mél : shollenbeck@verisign.com