

Groupe de travail réseau
Request for Comments : 2585
Catégorie : Normes

R. Housley
SPYRUS
IMC
May 1999

Traduction :
Julien MORLIERE
Mai 2005

Infrastructure Internet X.509 à clé publique Protocoles opérationnels: FTP et HTTP

Statut de cette note :

Ce document spécifie une norme Internet de protocole de voie pour la communauté Internet, et demande discussion et suggestions pour des améliorations.

Veillez vous référer à l'édition courante « Internet Official Protocol Standards » (STD 1) pour l'état de standardisation et le statut de ce protocole. La distribution de cette note est illimitée.

Notification de Copyright :

Copyright (C) The Internet Society (1999) Tous droits réservés.

En résumé :

Les conventions du protocole décrites dans ce document satisfont certaines des conditions opérationnelles de l'«Internet Public Key Infrastructure» (PKI) (Infrastructure Internet à clé publique)

Ce document indique les conventions pour l'usage du «File Transfer Protocol» (FTP) et du «Hypertext Transfer Protocol» (HTTP) pour obtenir les certificats et les «Certificate Revocation List» (CRL) (listes de révocation de certificat) des dépôts de PKI.

Des mécanismes additionnels concernant les conditions opérationnelles de PKIX sont indiqués dans des documents séparés.

1 Introduction :

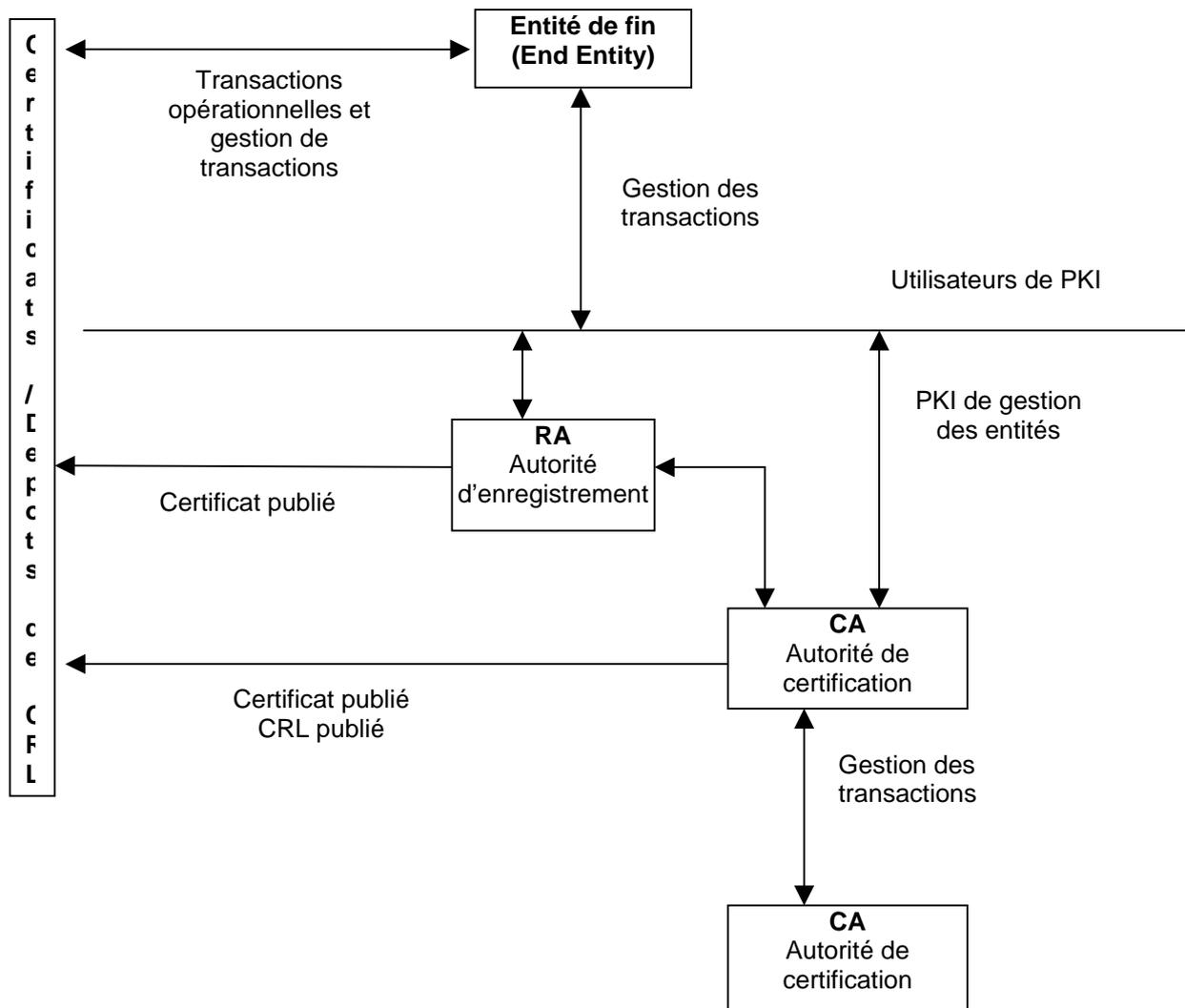
Cette spécification est une partie d'une norme à parties multiples pour les «Internet Public Key Infrastructure» (PKI) utilisant les certificats X.509 et les «certificate revocation lists» (CRL).

Ce document indique les conventions pour l'usage du File Transfer Protocol (FTP) et l'«Hypertext Transfer Protocol» (HTTP) pour obtenir des certificats et les CRL depuis les dépôts de PKI.

Des mécanismes additionnels concernant l'accès du dépôt de la PKI sont indiqués dans des documents séparés.

Modèle :

Ce qui suit est une vue simplifiée du modèle architectural assumé par les spécifications de l'Internet PKI.



Les composants dans ce modèle sont :

End Entity : utilisateur de certificats à PKI et/ou système d'utilisateur final qui est le sujet d'un certificat.

CA : Autorité de certification (certification authority)

RA : Autorité d'enregistrement (registration authority) Un système optionnel auquel la CA délègue certaines fonctions de gestion.

Dépôt : Un système ou une collection de systèmes répartis qui stockent les certificats et les CRL et sert à la manière d'un distributeur de ces certificats et CRL vers les destinataires finaux.

1.1. Certificat et dépôt de CRL :

Certaines autorités de certifications (CA) mandatent l'utilisation de services de validation en ligne, alors que d'autres distribuent les listes de certificats révoqués (CRL) pour permettre aux utilisateurs de certificat d'effectuer la validation de certificat par eux-mêmes.

Généralement les CA rendent les CRL disponibles aux utilisateurs de certificats en les éditant dans l'annuaire.

L'annuaire est également le mécanisme normal de distribution pour des certificats.

Cependant, les services d'annuaires ne sont actuellement que peu répandus sur Internet.

Le « File Transfer Protocol » (FTP) défini dans la RFC 959 et « the Hypertext Transfer Protocol » (HTTP) défini dans la RFC 2068 qui offrent des méthodes alternatives pour la certification et la distribution de CRL.

Les entités d'extrémités et les CA peuvent rechercher des certificats et des CRL depuis le dépôt en utilisant FTP ou HTTP.

Les entités d'extrémités peuvent éditer leur propre certificat dans le dépôt en utilisant FTP ou HTTP.

Les RA et CA peuvent éditer des certificats et des CRL dans le dépôt en utilisant FTP ou HTTP.

2 Conventions FTP :

Dans les extensions de certificat et de CRL, le formulaire d' « Uniform Resource Identifier » (URI) (identifiant de ressources universelles) de « GeneralName » est utilisé pour indiquer l'endroit où des émetteurs de certificats et de CRL peuvent être obtenus.

Par exemple, un URI identifiant le sujet d'un certificat peut être porté dans l'extension de certificat du « subjectAltName »

Un « IA5String » décrit l'utilisation de FTP en anonyme pour chercher le certificat ou l'information de la CRL.

Par exemple:

<ftp://ftp.netcom.com/sp/spyrus/housley.cer>

<ftp://ftp.your.org/pki/id48.cer>

<ftp://ftp.your.org/pki/id48.no42.crl>

Les utilisateurs d'Internet peuvent éditer la référence d'URI à un fichier qui contient leur certificat sur leur carte de visite professionnelle.

Cette pratique est utile quand il n'y a aucune entrée d'annuaire pour cet utilisateur.

Le FTP est largement déployé, et le FTP anonyme est accepté par beaucoup de pare-feu.

Ainsi, le FTP est une alternative attrayante aux protocoles d'accès d'annuaire pour le certificat et la distribution de CRL.

Tandis que ce service répond à l'exigence de recherche de l'information liée à un certificat qui est déjà identifié par un URI, on ne le prévoit pas pour satisfaire le problème plus général de recherche d'un certificat pour un utilisateur au sujet duquel une autre information, telle que son adresse de courrier électronique ou son affiliation de corporation, est connue.

Par commodité, les noms de fichiers qui contiennent des certificats devraient avoir un suffixe de type « .cer ».

Chaque dossier avec l'extension « .cer » contient exactement un certificat, encodé dans le format DER.

De même, les noms de fichiers qui contiennent des CRL devraient avoir un suffixe de type « .crl ».

Chaque fichier d'extension « .crl » contient exactement une CRL, encodé dans le format DER.

3 Conventions HTTP :

Dans les extensions de certificat et de CRL, la forme d'URI de « GeneralName » est utilisée pour indiquer l'endroit où des émetteurs de certificats et le CRL peuvent être obtenus.

Par exemple, un URI identifiant le sujet d'un certificat peut être porté dans l'extension de certificat de « subjectAltName »

Un « IA5String » décrit l'utilisation du HTTP pour chercher le certificat ou l'information de la CRL.

Par exemple :

<http://www.netcom.com/sp/spyrus/housley.cer>

<http://www.your.org/pki/id48.cer>

<http://www.your.org/pki/id48.no42.crl>

Les utilisateurs d'Internet peuvent éditer la référence d'URI à un fichier qui contient leur certificat sur leur carte de visite professionnelle.

Cette pratique est utile quand il n'y a aucune entrée d'annuaire pour cet utilisateur.

Le HTTP est largement déployé, et le HTTP accepté par beaucoup de pare-feu.

Ainsi, le HTTP est une alternative attrayante aux protocoles d'accès d'annuaire pour le certificat et la distribution de CRL.

Tandis que ce service répond à l'exigence de recherche d'information liée à un certificat qui est déjà identifié par un URI, on ne le prévoit pas pour satisfaire le problème plus général de recherche d'un certificat pour un utilisateur au sujet duquel une autre information, telle que son adresse de courrier électronique ou son affiliation de corporation, est connue.

Par commodité, les noms des fichiers qui contiennent des certificats devraient avoir un suffixe de type «.cer»

Chaque fichier avec l'extension «.cer» contient exactement un certificat, codé dans le format DER.

De même, les noms des fichiers qui contiennent des CRL devraient avoir un suffixe de type «.crl».

Chaque fichier avec une extension «.crl» contient exactement une CRL, encodé dans le format DER.

4 Enregistrements de MIME :

Deux types MIME sont définis pour supporter le transfert de certificats et de CRL.

Il y a :

application/pkix-cert

application/pkix-crl

4.1. application/pkix-cert :

A : ietf-types@iana.org

Sujet : Enregistrement d'application avec le type de média MIME/pkix-cert

Nom du type de média MIME : application

Nom du sous type MIME : pkix-cert

Paramètres requis : Aucun

Paramètres optionnels : version (Valeur par défaut : "1")

Considérations d'encodage : Il n'y en aura aucune pour des transports de 8 bits et très probablement pour « Base64 » pour SMTP et autres transports de 7 bits.

Considérations de sécurité : Porte un certificat cryptographique

Considérations d'interopérabilité: Aucune

Spécification éditée : draft-ietf-pkix-ipki-part1

Applications qui utilisent ce type de média : N'importe quel « MIME-complaint » de transport

Informations additionnelles :

Nombre(s) magique : Aucun

Extension(s) de fichiers : .CER

Code(s) des types de fichiers Macintosh : Aucun

Personne et Adresses email à contacter pour plus d'informations : Russ Housley
<housley@spyrus.com>

Usage attendu : COMMUN

Auteur/Contrôleur de changements : Russ Housley <housley@spyrus.com>

4.2. application/pkix-crl

A : ietf-types@iana.org

Sujet : Enregistrement d'application avec le type de média MIME/pkix-crl

Nom du type de média MIME : application

Nom du sous type MIME : pkix-crl

Paramètres requis : Aucun

Paramètres optionnels : version (Valeur par défaut : "1")

Considérations d'encodage : Il n'y en aura aucune pour des transports de 8 bits et très probablement pour « Base64 » pour SMTP et autres transports de 7 bits.

Considérations de sécurité : Porte une liste de révocation de certificat cryptographique

Considérations d'interopérabilité: Aucune

Spécification éditée : draft-ietf-pkix-ipki-part1

Applications qui utilisent ce type de média : N'importe quel « MIME-complaint » de transport

Informations additionnelles :

Nombre(s) magique : Aucun

Extension(s) de fichiers : . CRL Macintosh

Code(s) des types de fichiers : Aucun

Personne et Adresses email à contacter pour plus d'informations : Russ Housley
<housley@spyrus.com>

Usage attendu : COMMUN

Auteur/Contrôleur de changements : Russ Housley <housley@spyrus.com>

Références

[RFC 959] Postel, J. and J. Reynolds, «File Transfer Protocol (FTP)», STD 5, RFC 959, octobre 1985.

[RFC 1738] Berners-Lee, T., Masinter, L. and M. McCahill, «Uniform Resource Locators (URL)», RFC 1738, décembre 1994.

[RFC 2068] Fielding, R., Gettys, J., Mogul, J., Frystyk, H. and T. Berners-Lee; «Hypertext Transfer Protocol -- HTTP/1.1», RFC 2068, janvier 1997.

Considérations de sécurité :

Depuis que les certificats et les CRL sont numériquement signés, aucun service additionnel d'intégrité est nécessaire.

Ni les certificats ni les CRL n'ont besoin d'être gardés secrets, et l'accès anonyme aux certificats et aux CRL est généralement acceptable.

Ainsi, un service privé n'est nécessaire.

Le HTTP avec des proxy est fréquent sur l'Internet, et certains proxy ne vérifient pas la dernière version d'un objet correctement.

Si une demande HTTP de certificat ou de CRL passe par une configuration manquante ou par un proxy défaillant, le proxy peut renvoyer une réponse obsolète.

Les opérateurs de sites FTP et les serveurs du World Wide Web devraient authentifier les entités d'extrémité qui éditent des certificats aussi bien que les CA et les RA qui éditent des certificats et des CRL. Cependant, l'authentification n'est pas nécessaire pour rechercher des certificats et des CRL.

Adresse des auteurs :

Russell Housley
SPYRUS
381 Elden Street, Suite 1120
Herndon, VA 20170 USA
Email : housley@spyrus.com

Paul Hoffman
Internet Mail Consortium
127 Segre Place
Santa Cruz, CA 95060 USA
Email : phoffman@imc.org

Déclaration de Copyright :

Copyright (C) The Internet Society (2000). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis à des tiers, et les travaux dérivés qui le commentent ou l'expliquent ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou en partie, sans restriction d'aucune sorte, pourvu que la déclaration de copyright ci-dessus et le présent paragraphe soient inclus sur de telles copies et travaux dérivés.

Cependant, le présent document ne peut être modifié d'aucune façon, ni en retirant la déclaration de copyright ou les références à l' « Internet Society » ou à d'autres organisations Internet, excepté pour des besoins de développement de standards Internet.

Auquel cas les procédures de protection des droits de propriété intellectuelle définies dans le traitement des standards d'Internet doivent être suivies, ou autant que faire ce peut dans le cadre de traduction dans d'autres langues.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par l'Internet Society ni ses successeurs ou ayant-droits.

Le présent document et les informations qu'il contient sont fournies sur une base «EN L'ÉTAT» et L'INTERNET SOCIETY ET L'INTERNET ENGINEERING TASK FORCE DECLINENT TOUTE RESPONSABILITE, DIRECTE OU INDIRECTE ET SANS LIMITATION, QUANT AU FAIT QUE L'UTILISATION DES CES INFORMATIONS POURRAIT VIOLER DES DROITS OU DES GARANTIES IMPLICITES DE COMMERCIALISATION OU D'APTITUDE A UN BUT PARTICULIER.

Remerciement

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