Groupe de travail Réseau
Request for Comments : 5276
Catégorie : Sur la voie de la normalisation

C. Wallace, Cygnacom Solutions
août 2008
Traduction Claude Brière de L'Isle

Utilisation du protocole de validation de certificat fondé sur le serveur (SCVP) pour porter des enregistrements de preuve à long terme

Résumé
Le protocole de validation de certificat fondé sur le serveur (SCVP, *Server-based Certificate Validation Protocol*) définit un moyen extensible pour déléguer le développement et la validation de chemins de certification à un serveur. Il peut être utilisé pour prendre en charge le développement et la validation de chemins de certification bien après l'expiration des certificats dans le chemin en spécifiant un moment intéressant dans le passé. La syntaxe d'enregistrement de preuve (ERS, *Evidence Record Syntax*) définit des structures, appelées enregistrements de preuve, pour soutenir la non répudiation de l'existence des données. Les enregistrements de preuves peuvent être utilisés pour préserver des matériaux qui constituent un chemin de certification tel que la confiance dans les certificats puisse être établie après l'expiration des certificats dans le chemin et après que les algorithmes de chiffrement utilisés pour signer les certificats dans le chemin ne sont plus sûrs. Le présent document décrit l'usage du dispositif SCVP WantBack pour porter les enregistrements de preuves, permettant aux répondants à SCVP de fournir la préservation des preuves pour les certificats et les listes de révocation de certificats (CRL).

Table des matières

1. Introduction

Les signatures numériques sont fréquemment vérifiées en utilisant des dispositifs d'infrastructure de clé publique (PKI, *Public Key Infrastructure*) incluant des certificats de clé publique et des informations de révocation de certificat. Les vérificateurs construisent et valident les chemins de certification à partir d'un certificat de clé publique contenant la clé publique utilisée pour vérifier la signature auprès d'une clé publique de confiance. La construction d'un chemin de certification peut exiger l'acquisition de différents types d'informations générées par plusieurs PKI. Pour vérifier les

signatures numériques de nombreuses années après la génération de la signature, des considérations supplémentaires doivent être prises en compte. Par exemple, des dispositifs de PKI nécessaires peuvent n'être plus disponibles, certains peuvent avoir expiré, et les algorithmes ou clés de chiffrement utilisés pour générer les signatures numériques peuvent ne plus fournir le degré de sécurité désiré.

SCVP [RFC5055] donne le moyen de déléguer la construction et/ou validation du chemin de certification à un serveur, incluant la capacité de demander l'état d'un certificat par rapport à un instant dans le passé. SCVP ne définit pas de moyen de fournir ou valider des informations de non répudiation à long terme. ERS [RFC4998] définit une syntaxe pour préserver les matériaux sur de longues périodes par un régime qui inclut des re-signatures périodiques des matériaux pertinents en utilisant de nouvelles clés et des algorithmes de chiffrement plus forts. LTAP [LTANS-LTAP] définit un protocole pour communiquer avec un serveur d'archives à long terme (LTA, *Long-Term Archive*) pour les besoins de la préservation des enregistrements de preuves et des données. Les clients mémorisent, restituent, et suppriment les données en utilisant LTAP; les LTA maintiennent les enregistrements de preuves couvrant les données soumises par les clients.

Le présent document définit une application de SCVP pour permettre la restitution d'un enregistrement de preuve correspondant aux informations retournées par le serveur SCVP en créant une association entre un enregistrement de preuve et les informations contenues dans une réponse SCVP. La réponse SCVP peut alors être à son tour utilisée pour vérifier les objets de données archivés restitués en utilisant LTAP. Séparer la préservation des informations de chemin de certification de la préservation des données permet à la LTA de mémoriser les objets de données archivés de façon plus efficace, c'est-à-dire, les informations de vérification complètes n'ont pas besoin d'être mémorisées avec chaque objet de données archivé. Le vérificateur peut plus efficacement traiter les objets de données archivés en réutilisant les mêmes informations de chemin de certification pour vérifier plusieurs objets de données archivées d'époque similaire sans restituer et/ou valider plusieurs fois les mêmes dispositifs de PKI.

1.1 Notation des exigences

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. Concept des opérations

Durant le traitement du chemin de certification, les serveurs SCVP actifs peuvent rencontrer une large portion des dispositifs de PKI générés par une PKI particulière. En mémorisant et préservant ces dispositifs, un serveur SCVP peut répondre aux interrogations sur l'état d'un certificat sur de très longues périodes. Facultativement, les serveurs SCVP peuvent chercher activement des informations de PKI pour mémorisation et préservation, même quand aucune interrogation n'est faite, ce qui exige les informations durant leur période de validité afin de servir de futures interrogations à n'importe quel moment.

SCVP permet aux clients de demander autant d'information que désiré au serveur SCVP. Les clients incluent zéro, un ou plusieurs identifiants d'objet (OID, *Object Identifier*) indiquant le ou les types d'informations que le serveur devrait inclure dans la réponse. En définissant des valeurs d'OID supplémentaires, les clients peuvent demander un enregistrement de preuve (ER, *Evidence Record*) pour des types spécifiques d'informations retournés par le serveur SCVP. Le présent document définit des OID pour permettre la restitution des enregistrements de preuves pour les quatre types d'informations suivants :

- certificats d'entité d'extrémité,
- chemins de certification contenant un certificat d'entité d'extrémité jusqu'à une ancre de confiance,
- chemins de certification contenant un certificat intermédiaire jusqu'à une ancre de confiance,
- informations de révocation.

De plus, un OID est défini pour permettre l'inclusion d'un seul OID indiquant qu'un enregistrement de preuve est désiré pour toutes les informations demandées via le mécanisme WantBack *(retour voulu)*.

En associant des enregistrements de preuves à des informations maintenues par un serveur SCVP, les clients sont capables de déterminer l'état des certificats sur de très longues périodes en utilisant SCVP sans consulter de ressources supplémentaires. La nature des serveurs SCVP est bien adaptée à la préservation des matériaux d'infrastructure. De plus, la signature du serveur SCVP sur une réponse SCVP peut sécuriser la transmission des ancres de confiance incluses dans les enregistrements de preuves, permettant aux clients de s'abstenir d'établir des relations de confiance supplémentaires avec

les LTA.

Les transactions utilisées pour vérifier un objet de données archivé en utilisant LTAP et les WantBack SCVP décrits dans ce document sont les suivantes :
- o Le client restitue un objet de données archivé signé depuis un LTA en utilisant LTAP.
- o Le client prépare une demande SCVP pour valider le certificat du signataire au moment qui l'intéresse et inclut des WantBack pour les enregistrements de preuves correspondants aux dispositifs de PKI requis pour valider le certificat du signataire.
- o Le serveur SCVP retourne une réponse avec l'état au moment qui l'intéresse et inclut les enregistrements de preuves demandés.
- o Le client traite la demande SCVP, détermine l'état, et vérifie les enregistrements de preuves.
- o Le client vérifie les signatures dans l'objet de données archivé en utilisant le certificat du signataire validé.

3. Demandes

Les clients demandent des archives à long terme d'enregistrements de preuves à un serveur SCVP en incluant un des OID suivants dans le champ wantBack d'une CVRequest envoyée à un serveur SCVP :
- o id-swb-ers-best-cert-path
- o id-swb-ers-partial-cert-path
- o id-swb-ers-pkc-cert
- o id-swb-ers-revocation-info
- o id-swb-ers-all

De plus, id-swb-partial-cert-path est défini pour permettre aux clients de demander un chemin de certification partiel consistant en l'autorité de certification (CA, *Certification Authority*) qui a produit le certificat d'entité d'extrémité à travers une ancre de confiance. Ceci est similaire au WantBack id-swb-best-cert-path défini dans SCVP sauf que le replyWantBack résultant va contenir un CertBundle contenant le chemin de certification moins le certificat d'entité d'extrémité.

Pour chaque OID id-swb-ers sauf id-swb-ers-all, un EvidenceRecord (comme défini dans la [RFC4998]) couvrant les informations correspondantes dans la réponse va être retourné comme replyWantBack. Par exemple, si un client souhaite obtenir des informations de chemin de certification et de révocation plus un enregistrement de preuve pour chaque, la demande SCVP va inclure les quatre OID replyWantBack suivants : id-swb-best-cert-path, id-swb-pkc-revocation-info, id-swb-ers-best-cert-path, et id-swb-ers-revocation-info.

Autrement, pour id-swb-ers-all, une structure EvidenceRecordWantBacks va être retournée contenant un EvidenceRecord pour chaque élément d'information contenu dans le champ replyWantBacks. Par exemple, si un client souhaite obtenir un chemin de certification et des informations de révocation plus un enregistrement de preuve pour chaque, la demande SCVP pourrait inclure les trois OID replyWantBack suivants : id-swb-best-cert-path, id-swb-pkc-revocation-info, et id-swb-ers-all.

4. Réponses

Quand une demande de client contient une demande WantBack pour un enregistrement de preuve, la réponse générée DOIT inclure le replyWantBack contenant les informations demandées plus un replyWantBack contenant l'enregistrement de preuve correspondant à ces informations. Pour chaque OID id-swb-ers sauf id-swb-ers-pkc-cert et id-swb-ers-revocation-info, l'enregistrement de preuve DOIT être calculé sur la valeur du champ "value " dans le replyWantBack correspondant ; les octets d'étiquette et de longueur ne sont pas couverts par l'enregistrement de preuve. Les cibles pour les replyWantBack id-swb-ers-pkc-cert et id-swb-ers-revocation-info sont décrits ci-dessous. Par exemple, si la demande d'un client contient id-swb-pkc-best-cert-path et id-swb-ers-best-cert-path, la réponse résultante va contenir une replyWantBack de chaque type où l'enregistrement de preuve couvre le CertBundle codé en DER retourné dans la replyWantBack id-swb-pkc-best-cert-path. Pour id-swb-ers-pkc-cert, l'enregistrement de preuve DOIT être calculé sur la valeur du champ "cert" dans l'objet CertReply. Pour id-swb-ers-revocation-info, une séquence d'enregistrements de preuves est retournée. Chaque objet d'informations de révocation contenu dans la replyWantBack id-swb-pkc-revocation-info est couverte par un enregistrement de preuve dans la replyWantBack id-swb-ers-revocation-info. Un seul enregistrement de preuve peut couvrir plusieurs objets d'informations de révocation. L'enregistrement de preuve correct peut être identifié par la localisation du hachage de l'objet Informations de révocation dans le premier horodatage initial de l'enregistrement de

preuve.

Si le serveur ne peut pas retourner un EvidenceRecord pour l'élément d'information demandé, une replyWantBack du type approprié DOIT être retournée avec un champ de valeur vide. Par exemple, si un client demande id-swb-ers-pkc-cert et si le serveur ne peut pas satisfaire la demande, la réponse résultante va contenir une replyWantBack avec le champ "wb" réglé à id-swb-ers-pkc-cert et le champ "valeur" vide, c'est-à-dire, de longueur zéro.

5. WantBack

Les paragraphes qui suivent décrivent chaque WantBack défini dans ce document. Chaque WantBack pour un enregistrement de preuve exige un WantBack correspondant pour l'objet couvert par l'enregistrement de preuve qui doit être présent dans la demande. À réception d'une demande manquant du WantBack correspondant pour l'objet couvert par un enregistrement de preuve demandé, le serveur DOIT indiquer wantBackUnsatisfied dans le ReplyStatus. Les clients PEUVENT ignorer les WantBack d'enregistrement de preuve quand le WantBack pour l'objet correspondant n'est pas présent.

5.1 Enregistrement de preuve pour un chemin de certification complet

L'OID id-swb-ers-best-cert-path est utilisé pour demander un enregistrement de preuve pour un chemin de certification complet. Il est utilisé en conjonction avec l'OID id-swb-best-cert-path. Les demandes qui contiennent id-swb-ers-best-cert-path comme WantBack DOIVENT aussi contenir id-swb-best-cert-path. Les réponses qui contiennent id-swb-ers-best-cert-path DOIVENT aussi contenir id-swb-best-cert-path.

Un serveur SCVP peut maintenir des enregistrements de preuves pour des chemins de certification complets, c'est-à-dire, des chemins de certification qui contiennent tous les certificats de l'entité d'extrémité à l'ancre de confiance. L'enregistrement de preuve DOIT être calculé sur le CertBundle retourné via le replyWantBack id-swb-best-cert-path. Dans ce cas, une signature dans l'objet de données archivé peut être vérifiée en utilisant un certificat d'entité d'extrémité retourné via SCVP. Le certificat d'entité d'extrémité peut être vérifié en utilisant SCVP avec une demande contenant id-swb-ers-best-cert-path, id-swb-best-cert-path, id-swb-pkc-revocation-info, et id-swb-ers-revocation-info.

5.2 Enregistrement de preuve pour un chemin de certification partiel

L'OID id-swb-ers-partial-cert-path est utilisé pour demander un enregistrement de preuve pour un chemin de certification partiel. Il est utilisé conjointement avec l'OID id-swb-partial-cert-path. Les demandes qui contiennent id-swb-ers-partial-cert-path comme WantBack DOIVENT aussi contenir id-swb-partial-cert-path. Les réponses qui contiennent id-swb-ers-partial-cert-path DOIVENT aussi contenir id-swb-partial-cert-path.

Comme solution de remplacement à l'utilisation de SCVP pour obtenir des enregistrements de preuves pour des certificats d'entité d'extrémité, le certificat pourrait être inclus dans le ou les objets de données archivés soumis à un LTA. Dans ce cas, une signature dans l'objet de données archivé peut être vérifiée en utilisant le certificat d'entité d'extrémité inclus, qui est protégé par l'enregistrement de preuve couvrant l'objet de données archivé, incluant le certificat. Le certificat d'entité d'extrémité peut être vérifié en utilisant SCVP avec une demande contenant id-swb-partial-cert-path, id-swb-ers-partial-cert-path, id-swb-pkc-revocation-info, et id-swb-ers-revocation-info. À la différence du chemin de certification partiel, les informations de révocation incluent du matériel qui peut être utilisé pour déterminer l'état du certificat d'entité d'extrémité.

En maintenant un enregistrement de preuve pour un chemin de certification partiel, les serveurs SCVP peuvent réaliser une meilleure efficacité de mémorisation.

5.3 Enregistrement de preuve pour un certificat de clé publique

L'OID id-swb-ers-pkc-cert est utilisé pour demander un enregistrement de preuve pour certificat individuel de clé publique. Il est utilisé en conjonction avec l'OID id-swb-pkc-cert. Les demandes qui contiennent id-swb-ers-pkc-cert comme WantBack DOIVENT aussi contenir id-swb-pkc-cert. Les réponses qui contiennent id-swb-ers-pkc-cert DOIVENT aussi contenir id-swb-pkc-cert. Les serveurs SCVP peuvent maintenir des enregistrements de preuves pour des certificats individuels. Cela permet aux clients d'omettre le certificat du signataire de l'objet de données archivé soumis à un LTA. Dans ce cas, une signature dans l'objet de données archivé peut être vérifiée en utilisant un certificat d'entité d'extrémité retourné via SCVP. Le certificat d'entité d'extrémité peut être vérifié en utilisant SCVP avec une demande contenant id-

swb-pkc-cert, id-swb-ers-pkc-cert, id-swb-partial-cert-path, id-swb-ers-partial-cert-path, id-swb-pkc-revocation-info, et id-swb-ers-revocation-info.

5.4 Enregistrement de preuve pour informations de révocation

L'OID id-swb-ers-revocation-info est utilisé pour demander des enregistrements de preuves pour un ensemble d'informations de révocation. Il est utilisé en conjonction avec l'OID id-swb-revocation-info. Les demandes qui contiennent id-swb-ers-revocation-info comme WantBack DOIVENT aussi contenir id-swb-revocation-info. Les réponses qui contiennent id-swb-ers-revocation-info DOIVENT aussi contenir id-swb-revocation-info. Une séquence d'enregistrements de preuves est retournée, avec un enregistrement de preuve pour chaque élément dans id-swb-revocation-info.

```
EvidenceRecords ::= SEQUENCE TAILLE (1..MAX) DE EvidenceRecord
```

Un serveur SCVP peut maintenir des enregistrements de preuves pour des informations de révocation. Les informations de révocation peuvent être fournies sous la forme de CRL ou de réponses du protocole d'état de révocation en ligne (OCSP, *Online Certificate Status Protocol*). Des CRL cumulatives peuvent être générées pour archivage pour simplifier la maintenance des enregistrements de preuve.

5.5 Enregistrement de preuve pour tout replyWantBack

Un serveur SCVP peut maintenir des enregistrements de preuves pour des types d'informations supplémentaires qui peuvent être retournées en utilisant le mécanisme wantBack, par exemple, des informations de certificat d'attribut. L'OID id-swb-ers-all fournit un moyen abrégé pour que les clients demandent des enregistrements de preuves pour toutes les informations retournées via le champ replyWantBacks. Comme id-swb-ers-all peut résulter en le retour de plusieurs enregistrements de preuves dans la réponse, un mécanisme est nécessaire pour associer un enregistrement de preuve au type d'informations couvertes par l'enregistrement de preuve. La structure EvidenceRecordWantBacks fournit un moyen souple de porter un enregistrement de preuve pour différents types d'informations.

```
EvidenceRecordWantBack ::= SEQUENCE  {
   targetWantBack    IDENTIFIANT D'OBJET ,
   evidenceRecord    EvidenceRecord FACULTATIF
}

EvidenceRecordWantBacks ::= SEQUENCE TAILLE (1..MAX) DE EvidenceRecordWantBack
```

EvidenceRecordWantBacks est une SEQUENCE DE structures EvidenceRecordWantBack. Le champ targetWantBack indique le type de replyWantBack couvert par le EvidenceRecord associé. Le champ evidenceRecord, si il est présent, contient une structure EvidenceRecord calculée sur le replyWantBack indiqué par le champ targetWantBack. Lorsque EvidenceRecordWantBacks est utilisé, il DOIT y avoir une correspondance biunivoque entre les autres objets replyWantBack et les objets dans la collection EvidenceRecordWantBacks. Si un serveur n'a pas de EvidenceRecord pour un objet replyWantBack particulier, un EvidenceRecordWantBack avec le champ evidenceRecord absent devrait être inclus dans la collection EvidenceRecordWantBacks.

5.6 Chemin de certification partiel

L'OID id-swb-partial-cert-path est une solution de remplacement de id-swb-best-cert-path. C'est le seul OID défini dans ce document pour lequel un EvidenceRecord n'est pas retourné dans la réponse. Pour l'efficacité, les serveurs SCVP qui maintiennent des enregistrements de preuves pour les chemins de certification peuvent seulement le faire pour des chemins partiels au lieu de maintenir un ou plusieurs chemins pour chaque certificat d'entité d'extrémité.

Les clients SCVP peuvent inclure un id-swb-partial-cert-path dans une demande quand un chemin de certification partiel est exigé. Cela va être normalement inclus avec un id-swb-ers-partial-cert-path pour tenir compte du fait que certains serveurs SCVP produisent seulement des enregistrements de preuves pour des chemins partiels pour des raisons de mémorisation et d'efficacité de calcul. Dans ce cas, un enregistrement de preuve séparé peut être disponible pour le certificat d'entité d'extrémité en incluant id-swb-pkc-cert et id-swb-ers-pkc-cert dans la demande.

6. Considérations sur la sécurité

Pour les considérations de sécurité spécifiques de SCVP, voir la [RFC5055]. Pour les considérations de sécurité spécifiques de ERS, voir la [RFC4998].

La signature sur la réponse SCVP contenant une ou plusieurs structures ERS doit être vérifiée en utilisant une clé publique de confiance pour le consommateur d'assertions. La réponse peut contenir des ancres de confiance utilisées pour vérifier les couches intérieures d'une structure ERS. Les ancres de confiance sont protégées par la signature du serveur SCVP couvrant la réponse. Le consommateur d'assertions peut choisir d'utiliser les ancres de confiance portées dans la réponse ou ignorer les ancres de confiance en faveur des ancres de confiance restituées hors bande. Les consommateurs d'assertions DEVRAIENT ignorer les ancres de confiance contenues dans des réponses SCVP non signées.

7. Références

7.1 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)

[RFC4998] T. Gondrom et autres, "Syntaxe d'enregistrement de preuve (ERS)", août 2007. *(P.S.)*

[RFC5055] T. Freeman et autres, "Protocole de validation de certificat fondée sur le serveur (SCVP)", décembre 2007. *(P.S.)*

7.2 Références pour information

[LTANS-LTAP] Jerman-Blazic, A., Sylvester, P., and C. Wallace, "Long-term Archive Protocol (LTAP)", Travail en cours, février 2008.

Appendice A. Module ASN.1

Le module ASN.1 suivant définit les identifiants d'objets utilisés pour identifier six nouvelles formes de WantBack SCVP et trois nouvelles structures. EvidenceRecordWantBack et EvidenceRecordWantBacks sont utilisés en conjonction avec le WantBack id-swb-ers-all pour corréler les enregistrements de preuve avec des WantBack. EvidenceRecords est utilisé en conjonction avec le WantBack id-swb-ers-revocation-info pour retourner des enregistrements de preuve pour les objets d'information de révocation individuels.

```
LTANS-SCVP-EXTENSION { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) ltans(11) id-mod(0) id-mod-ers-scvp(5) id-mod-ers-scvp-v1(1) }

ÉTIQUETTES IMPLICITES DE DÉFINITIONS ::=
DÉBUT

IMPORTE

id-swb
FROM SCVP
{ iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) 21 }

EvidenceRecord
FROM ERS
{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) ltans(11) id-mod(0) id-mod-ers88(2) id-mod-ers88-v1(1) };

IDENTIFIANT D'OBJET id-swb-partial-cert-path ::= {id-swb 15 }
```

```
IDENTIFIANT D'OBJET id-swb-ers-pkc-cert ::= {id-swb 16 }
IDENTIFIANT D'OBJET id-swb-ers-best-cert-path ::= {id-swb 17 }
IDENTIFIANT D'OBJET id-swb-ers-partial-cert-path ::= {id-swb 18 }
IDENTIFIANT D'OBJET id-swb-ers-revocation-info ::= {id-swb 19 }
IDENTIFIANT D'OBJET id-swb-ers-all ::= {id-swb 20 }

EvidenceRecordWantBack ::= SEQUENCE
{
   targetWantBack    IDENTIFIANT D'OBJET ,
   evidenceRecord    EvidenceRecord FACULTATIF
}

EvidenceRecordWantBacks ::= SEQUENCE TAILLE (1..MAX) DE EvidenceRecordWantBack

EvidenceRecords ::= SEQUENCE TAILLE (1..MAX) DE EvidenceRecord

FIN
```

Adresse de l'auteur

Carl Wallace
Cygnacom Solutions
Suite 5200
7925 Jones Branch Drive
McLean, VA 22102
mél : cwallace@cygnacom.com

Déclaration complète de droits de reproduction

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