Groupe de travail Réseau
**Request for Comments : 4557**
**Catégorie : Sur la voie de la normalisation**
Traduction Claude Brière de L'Isle

L. Zhu, Microsoft Corporation
K. Jaganathan, Microsoft Corporation
N. Williams, Sun Microsystems
juin 2006

# Prise en charge du protocole d'état de certificat en ligne (OCSP) pour la cryptographie à clé publique pour l'authentification initiale dans Kerberos (PKINIT)



**Résumé**
Le présent document définit un mécanisme pour permettre la transmission dans la bande des réponses du protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol*) dans le protocole Kerberos d'authentification du réseau. Ces réponses sont utilisées pour vérifier la validité des certificats utilisés dans le chiffrement à clé publique pour l'authentification initiale dans Kerberos (PKINIT, *Public Key Cryptography for Initial Authentication in Kerberos*), qui est l'extension à Kerberos Version 5 qui s'occupe de l'utilisation du chiffrement à clé publique.

## Table des matières



## 1. Introduction

Le protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol*) [RFC2560] permet aux applications d'obtenir des informations à jour concernant l'état de révocation d'un certificat. Comme les réponses OCSP sont bien encadrées et de petite taille, les clients qui subissent des contraintes peuvent souhaiter utiliser OCSP pour vérifier la validité des certificats pour le centre de distribution de clés (KDC, *Key Distribution Center*) Kerberos afin d'éviter la transmission de grosses listes de révocation de certificats (CRL, *Certificate Revocation List*) et donc économiser la bande passante sur les réseaux à contraintes [RFC5019].

Le présent document définit un type de pré authentification [RFC4120], où le client et le KDC PEUVENT porter les réponses OCSP pour les certificats utilisés dans les échanges d'authentification, comme défini dans la [RFC4556].

En utilisant cette extension FACULTATIVE, les clients PKINIT et le KDC peuvent maximiser la réutilisation des réponses OCSP mises en antémémoire.

## 2. Conventions utilisées dans ce document

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].

## 3. Définition du message

Un identifiant de type de pré authentification est défini pour ce mécanisme :

PA-PK-OCSP-RESPONSE : 18

Le champ correspondant de padata-value *(valeur de données de pré authentification)* [RFC4120] contient le codage DER [X690] du type ASN.1 suivant :

PKOcspData ::= SEQUENCE DE OcspResponse
-- Si plus d'une OcspResponse est incluse, la première OcspResponse DOIT contenir la réponse OCSP pour le certificat du signataire. Le signataire se réfère respectivement au client pour AS-REQ, et au KDC pour AS-REP.

OcspResponse ::= CHAINE D'OCTETS
– Contient une réponse OCSP complète, comme défini dans la [RFC2560].

Le client PEUT envoyer des réponses OCSP pour les certificats utilisés dans PA-PK-AS-REQ [RFC4556] via une PA-PK-OCSP-RESPONSE.

Le KDC qui reçoit une PA-PK-OCSP-RESPONSE DEVRAIT envoyer une PA-PK-OCSP-RESPONSE contenant des réponses OCSP pour les certificats utilisés dans la PA-PK-AS-REP du KDC. Le client peut demander une PA-PK-OCSP-RESPONSE en utilisant une PKOcspData contenant une séquence vide.

Le KDC PEUT envoyer une PA-PK-OCSP-RESPONSE quand il ne reçoit pas de PA-PK-OCSP-RESPONSE du client.

La PA-PK-OCSP-RESPONSE envoyée par le KDC contient des réponses OCSP pour les certificats utilisés dans la PA-PK-AS-REP [RFC4556].

Noter le manque de protection de l'intégrité pour la réponse OCSP vide ou manquante ; le manque d'une réponse OCSP attendue du KDC pour les certificats de KDC DEVRAIT être traité comme une erreur par le client, sauf si il est configuré autrement.

Quand on utilise OCSP, la réponse est signée par le serveur OCSP, qui est de confiance pour le receveur. Selon la politique locale, d'autres vérifications de la validité des serveurs OCSP peuvent être nécessaires.

Le client et le KDC DEVRAIENT ignorer les réponses OCSP invalides reçues via ce mécanisme, et ils PEUVENT mettre en œuvre la logique de traitement de CRL comme position de repli, si les réponses OCSP reçues via ce mécanisme seul sont insuffisantes pour la vérification de la validité du certificat. Le client et/ou le KDC PEUVENT ignorer une réponse OCSP valide et effectuer indépendamment leur propre vérification d'état de révocation.

## 4. Considérations sur la sécurité

Les données de pré authentification dans le présent document n'authentifient en fait aucun principal, mais sont conçues pour être utilisées conjointement à PKINIT.

Il n'y a pas de lien entre les données de pré authentification PA-PK-OCSP-RESPONSE et les données de pré authentification PKINIT autres qu'une certaine réponse OCSP correspondant à un certificat utilisé dans un élément de données de pré authentification PKINIT. Les attaques qui impliquent la suppression ou le remplacement d'éléments de données de pré authentification PA-PK-OCSP-RESPONSE sont, au pire, des attaques en dégradation, où un client PKINIT ou un KDC va poursuivre sans utiliser de CRL ou OCSP pour la validation de certificat, ou des attaques de déni de service,

où un client PKINIT ou un KDC qui ne peut pas valider le certificat de l'autre sans la réponse OCSP qui l'accompagne pourrait rejeter l'échange d'AS ou pourrait avoir à télécharger de très grosses CRL afin de continuer. Kerberos V5 ne protège pas contre les attaques de déni de service ; donc, l'aspect déni de service de ces attaques est acceptable.

Si un client PKINIT ou un KDC ne peut pas valider les certificats sans l'aide d'une PA-PK-OCSP-RESPONSE valide, il DEVRAIT alors faire échouer l'échange d'AS, éventuellement en accord avec la configuration locale.

## 5. Remerciements

Le présent document se fonde sur des conversations entre les auteurs, Jeffrey Altman, Sam Hartman, Martin Rex, et d'autres membres du groupe de travail Kerberos.

## 6. Références

### 6.1 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)

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin et C. Adams, "Protocole d'état de certificat en ligne d'infrastructure de clé publique X.509 pour l'Internet - OCSP", juin 1999. *(P.S.) (Remplacée par* RFC6960)

[RFC4120] C. Neuman et autres, "Service Kerberos d'authentification de réseau (V5)", juillet 2005. (*MàJ par* RFC4537, 5021, 6649, 7751, 8062, 8129, 8429)

[RFC4556] L. Zhu, B. Tung, "Cryptographie à clé publique pour authentification initiale dans Kerberos (PKINIT)", juin 2006. *(P.S. ; MàJ par* RFC8062)

[X690] Recommandation UIT-T X.690, "ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", (1997) aussi Norme internationale ISO/CEI 8825-1:1998.

### 6.2 Référence pour information

[RFC5019] A. Deacon, R. Hurst, "Profil du protocole léger d'état de certificat en ligne (OCSP) pour environnements de gros volumes", septembre 2007. *(P.S.)*

## Adresse des auteurs

Larry Zhu
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US
mél : lzhu@microsoft.com

Karthik Jaganathan
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US
mél : karthikj@microsoft.com

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US
mél : Nicolas.Williams@sun.com

## Déclaration complète de droits de reproduction

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