

Groupe de travail Réseau  
**Request for Comments : 5179**  
 Catégorie : Sur la voie de la normalisation  
 Traduction Claude Brière de L'Isle

N. Williams, Sun  
 mai 2008

# Transposition des noms de service fondés sur le domaine d'interface de programme d'application de service générique de sécurité (GSS-API) pour le mécanisme GSS de Kerberos 5

## Statut du présent mémoire

Le présent document spécifie un protocole Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

## Résumé

Le présent document décrit la transposition des noms principaux de service fondés sur le domaine d'interface de programme d'application de service générique de sécurité (GSS-API, *Generic Security Service Application Program Interface*) en noms principaux de Kerberos 5.

## Table des Matières

1. Noms fondés sur le domaine pour le mécanisme GSS-API Kerberos 5.....	1
2. Conventions utilisées dans ce document.....	1
3. Considérations d'internationalisation.....	2
4. Exemples.....	2
5. Considérations sur la sécurité.....	2
6. Références normatives.....	2
Adresse de l'auteur.....	2
Déclaration complète de droits de reproduction.....	3

## 1. Noms fondés sur le domaine pour le mécanisme GSS-API Kerberos 5

En accord avec la [RFC5178], le présent document donne les détails spécifiques du mécanisme nécessaires pour mettre en œuvre les noms de service fondés sur le domaine de GSS-API [RFC2743] avec le mécanisme GSS-API de Kerberos 5 [RFC4121].

Le nom GSS\_C\_NT\_DOMAINBASED\_SERVICE DEVRAIT être transposé en nom principal Kerberos 5 comme suit :

- o le nom de <service> devient le premier composant du nom principal Kerberos 5 ;
- o le <nom d'hôte> devient le second composant du nom principal Kerberos 5 ;
- o le nom de <domaine> devient le troisième composant du nom principal Kerberos 5 ;
- o le domaine du nom principal résultant est celui qui correspond au nom de domaine, traité comme un nom d'hôte.

Les mêmes considérations et méthodes de canonisation de nom qu'utilisées ailleurs dans le mécanisme GSS-API de Kerberos 5 [RFC4121] et dans Kerberos 5 [RFC4120] en général s'appliquent ici.

Les mises en œuvre DEVRAIENT utiliser un type de nom Kerberos 5 de NTT-SRVT-HST-DOMAIN (qui a la valeur 12) mais PEUVENT utiliser à la place NT-UNKNOWN.

## 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. Considérations d'internationalisation

La meilleure façon de traiter l'internationalisation des noms principaux fondés sur le domaine de Kerberos 5 n'est pas claire pour l'instant, parce que le projet d'internationalisation du cœur du protocole Kerberos 5 n'est pas achevé.

Cependant, il est clair que la meilleure façon d'interopérer quand on utilise des noms principaux fondés sur le domaine de Kerberos 5 est d'utiliser des noms de domaine internationalisés codés en ACE [RFC3490] pour les créneaux de nom d'hôte et de domaine d'un nom principal fondé sur le domaine de Kerberos 5. Donc, les mises en œuvre de mécanisme GSS-API Kerberos 5 DOIVENT juste faire cela.

### 4. Exemples

- o Le nom fondé sur le domaine, de forme générique, "ldap@foo.exemple@ds1.foo.exemple" peut se transposer en un nom principal Kerberos 5 comme : "ldap/ds1.foo.exemple/ foo.exemple@FOO.EXEMPLE"
- o Le nom fondé sur le domaine, de forme générique, "kadmin@foo.exemple@kdc1.foo.exemple" peut se transposer en un nom principal Kerberos 5 comme : "kadmin/kdc1.foo.exemple/foo.exemple@FOO.EXEMPLE"

### 5. Considérations sur la sécurité

Voir la [RFC5178]. Il est important pour la sécurité des protocoles qui utilisent le mécanisme GSS-API de Kerberos 5 et les noms fondés sur le domaine, que le domaine des noms principaux fondés sur le domaine soit dérivé du nom d'hôte plutôt que du créneau de nom de domaine de la chaîne d'entrée du nom fondé sur le domaine.

### 6. 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](#))
- [RFC2743] J. Linn, "[Interface générique de programme d'application](#) de service de sécurité, version 2, mise à jour 1", janvier 2000. (MàJ par [RFC5554](#))
- [RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (Remplacée par les RFC [5890](#) et [5891](#), P.S.)
- [RFC4120] C. Neuman et autres, "[Service Kerberos d'authentification de réseau](#) (V5)", juillet 2005. (MàJ par [RFC4537](#), [5021](#), [6649](#), [7751](#), [8062](#), [8129](#), [8429](#))
- [RFC4121] L. Zhu et autres, "Version 2 du [mécanisme d'interface de programme d'application](#) de service de sécurité générique (GSS-API) de Kerberos version 5", juillet 2005. (MàJ [RFC1964](#)) (MàJ par les [RFC6542](#), [6649](#), [8062](#))) (P.S.)
- [RFC5178] N. Williams, A. Melnikov, "[Internationalisation des noms de service](#) fondés sur le domaine et type de nom d'interface de programme d'application de service générique de sécurité (GSS-API)", mai 2008. (P.S.)

### Adresse de l'auteur

Nicolas Williams  
Sun Microsystems  
5300 Riata Trace Ct.  
Austin, TX 78727  
US

mél : [Nicolas.Williams@sun.com](mailto:Nicolas.Williams@sun.com)

## **Déclaration complète de droits de reproduction**

Copyright (C) The IETF Trust (2008).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### **Propriété intellectuelle**

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).