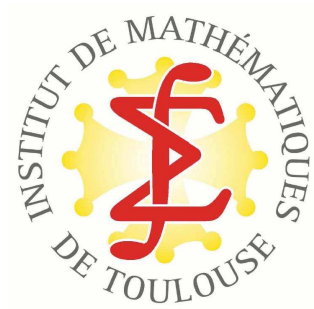
Kerberos: authentification unique

Linux®, Windows®, NetBSD®

David Bonnafous

david.bonnafous@math.ups-tlse.fr

Institut de Mathématiques de Toulouse



Remerciements

- Patrice, David et Miloslav (la cellule informatique)
- Guilhem Petit (stagiaire de l'Afpa encadré par Patrice)

Objectifs

1. avoir un seul mot de passe pour s'authentifier sous Windows et Linux (une seule base de données)
2. taper le mot de passe une seule fois par jour... (Single Sign-On)

Plan de la présentation

- Kerberos en bref
- Kerberos et Microsoft Windows
- Kerberos et UNIX/Linux
- Cross realm authentication
- Approbation de domaines
- Difficultés et perspectives

Kerberos en bref

- système d'authentification pour des systèmes en réseau ouvert
- première apparition en 1988 [4]
- Kerberos 4, première version utilisable
- Kerberos 5, RFC 4120, juillet 2005 (RFC 1510, septembre 1993)
- Kerberos 5 est utlisé dans
  - Microsoft Windows (2000, XP,...),
  - "UNIX" : Mac OS X, Linux, *BSD,
  - GSS-API, SASL (NFSv4, AFS, LDAP, SSH)
- beaucoup de doc : [3], [1], [2]

Kerberos en bref : bibliographie

Références

[1] Jason Garman. *Kerberos : The Definitive Guide*. O'Reilly, 2003.

[2] John T. Kohl, B. Clifford Neuman, and Theodore Y. Ts'o. The evolution of the kerberos authentication service. In *Proceedings of the Spring 1991 EurOpen Conference*, "1991",.

[3] Emmanuel le Chevoir. Étude de kerberos 5. Technical report, Hervé Schauer Consultants.

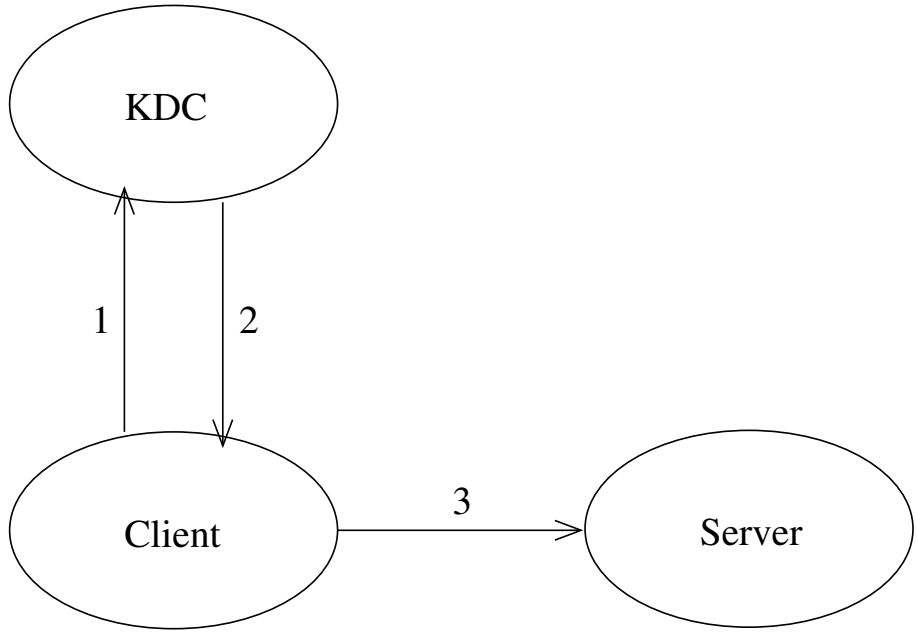
[4] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos : an authentication service for open network systems. In *Proceedings of the winter 1988 USENIX conference*, February 1988.

http ://www.kerberos.isi.edu/

Kerberos en bref : principe

- sûr,
- Single Sign-On,
- serveur tiers (le KDC qui connait le secret de tous les principaux),
- authentification mutuelle (client et serveur),

Kerberos en bref : principe[2]



1. Client $\rightarrow$ KDC : c, s, n
2. KDC $\rightarrow$ Client : $\{K_{c,s}, n\}K_c, \{T_{c,s}\}K_s$
3. Client $\rightarrow$ Server : $\{A_c\}K_{c,s}, \{T_{c,s}\}K_s$

Kerberos en bref : passwd

- le RFC 4120 ne définit pas de protocole pour changer le mot de passe
- “kpasswd” protocol, version 1 (historique)
- l’IETF travaille à le définir (draft d’octobre 2005)
- Microsoft a défini le sien : RFC 3244

Kerberos et Microsoft Windows

utilisé à partir de w2k [1]

- extension propriétaire PAC
- RFC 3244 pour le changement de mot de passe (ou un autre...)

  Description of password-change protocols in Windows 2000 != RFC 3244

Kerberos et Microsoft Windows

Références

[1] Microsoft TechNet. Windows 2000 kerberos authentication.

Kerberos 5 et UNIX/Linux

- shishi, Free Software Fundation
- MIT krb5
- Heimdal, KTH, Institut Royal de Technologie (Suède)
- module PAM
- Cyrus SASL -> GSS-API -> Kerberos 5

Cross realm authentication

- confiance mutuelle (ou pas) entre 2 royaumes Kerberos
- ex : passer d'une machine de l'institut de Toulouse à une machine de Mathrice sans se ré-authentifier
- -> création de clès inter-domaines

Kerberos, UNIX et Windows ? ? ? [2] [1]

Références

[1] Microsoft TechNet. Step-by-step guide to kerberos (krb5 1.0 interoperability. January 2000.

[2] Assar Westerlund and Johan Danielsson. Heimdal and windows 2000 kerberos : How to get them to play together. In *Proceedings of the FREENIX Track*. The USENIX Association, 2001.

- Client Windows dans un royaume Kerberos
- Client UNIX dans un domaine (“royaume”) AD
- Client d’AD et KDC UNIX (domaine AD = royaume Kerberos UNIX)
- approbation de domaines AD/royaume Kerberos

Windows dans un royaume Kerberos

- commande ksetup.exe (en ligne de commande ☺)
- dans les “Support Tools” de Windows

```
ksetup /setdomain UPS-TLSE.FR
ksetup /addkdc UPS-TLSE.FR pif.math.cnrs.fr
ksetup /mapuser dbonnafo@UPS-TLSE.FR david
```

➥ dbonnafo@UPS-TLSE.FR authentifié sur le KDC pif.math.cnrs.fr sera connecté sur la machine en tant que david.

```
ksetup /mapuser * *
```

UNIX dans un royaume AD

- qui voudrait faire ça ?
- Vintela™, *“One solution to consolidate, centralize, and integrate UNIX and Linux with Microsoft”*

➥ modules PAM propriétaires

AD et KDC UNIX

- avoir un seul royaume Kerberos pour AD et UNIX
- utiliser les KDC UNIX et pas celui de Windows

AD et KDC UNIX

- avoir un seul royaume Kerberos pour AD et UNIX
- utiliser les KDC UNIX et pas celui de Windows

IMPOSSIBLE ☹

Approbation de domaines

confiance entre un domaine AD et un royaume Kerberos

krbtgt/DOMAINE.AD@ROYAUME.KERBEROS
krbtgt/ROYAUME.KERBEROS@DOMAINE.AD

Approbation de domaines

confiance entre un domaine AD et un royaume Kerberos

krbtgt/DOMAINE.AD@ROYAUME.KERBEROS
krbtgt/ROYAUME.KERBEROS@DOMAINE.AD

sur le contrôleur de domaine

- Programs/Administrative tools/AD Domains and Trusts
- Properties/Trust/Add

Approbation de domaines

confiance entre un domaine AD et un royaume Kerberos

krbtgt/DOMAINE.AD@ROYAUME.KERBEROS
krbtgt/ROYAUME.KERBEROS@DOMAINE.AD

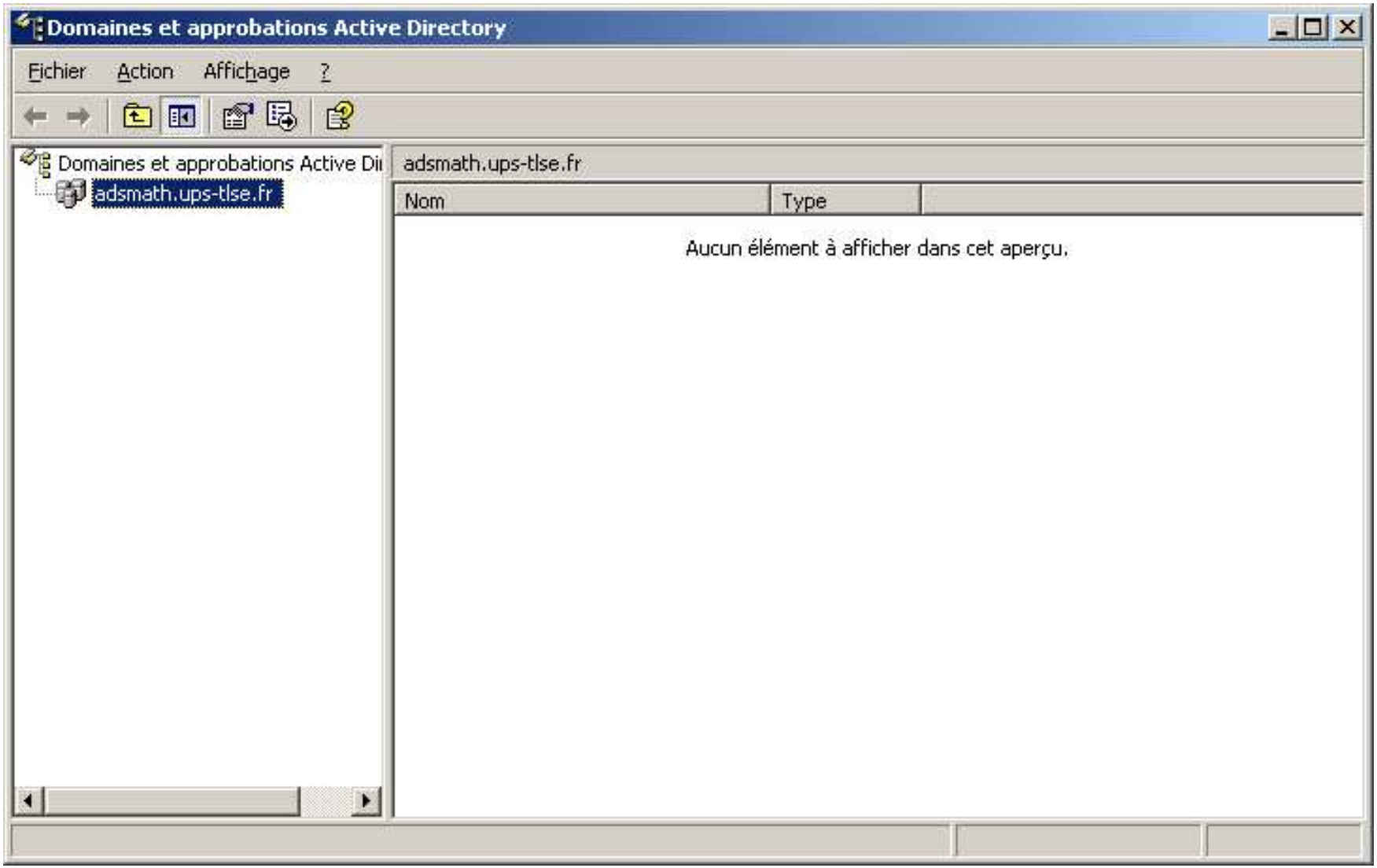
sur le contrôleur de domaine

- Programs/Administrative tools/AD Domains and Trusts
- Properties/Trust/Add

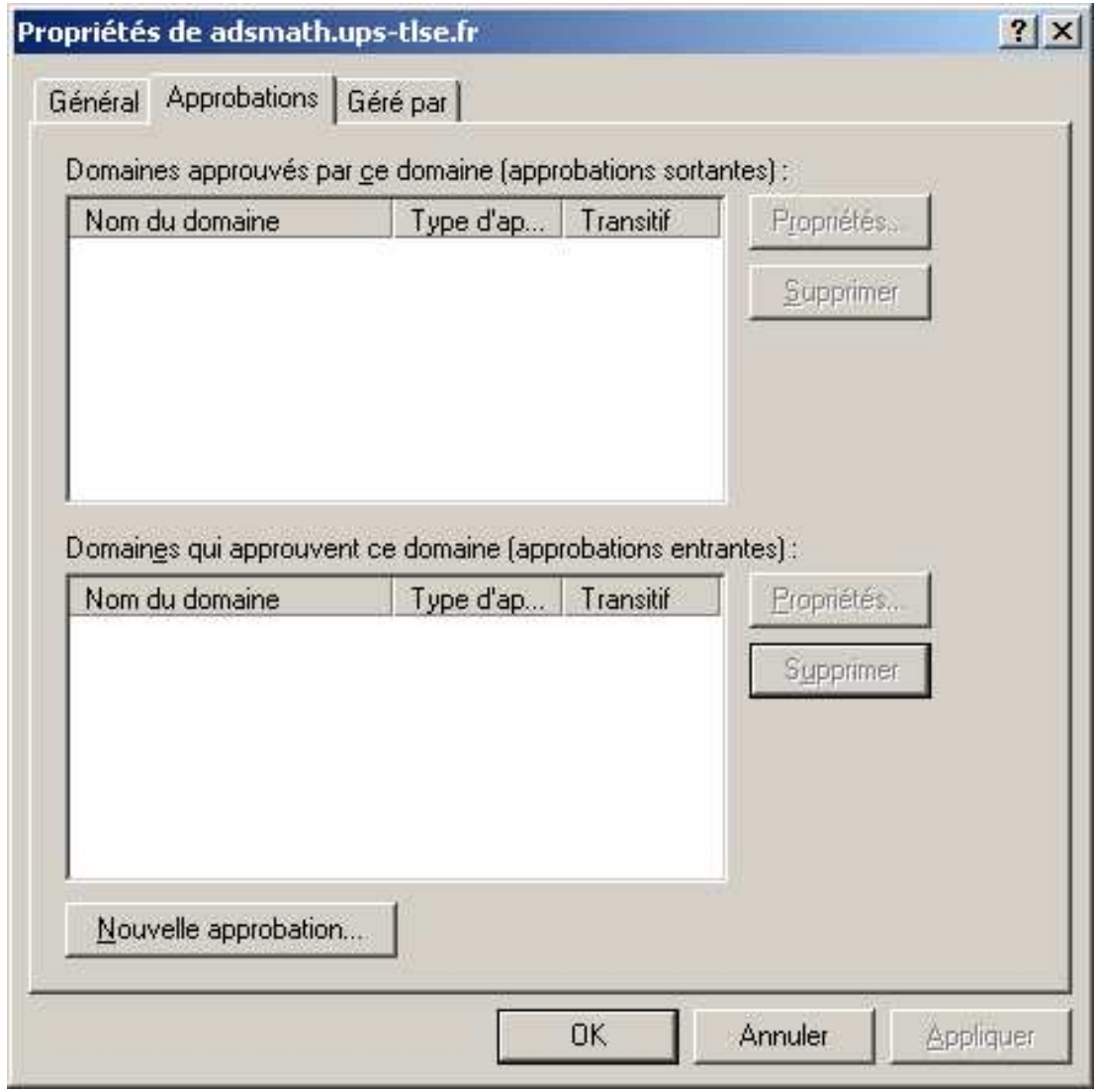
sur le KDC

- commande kadmin

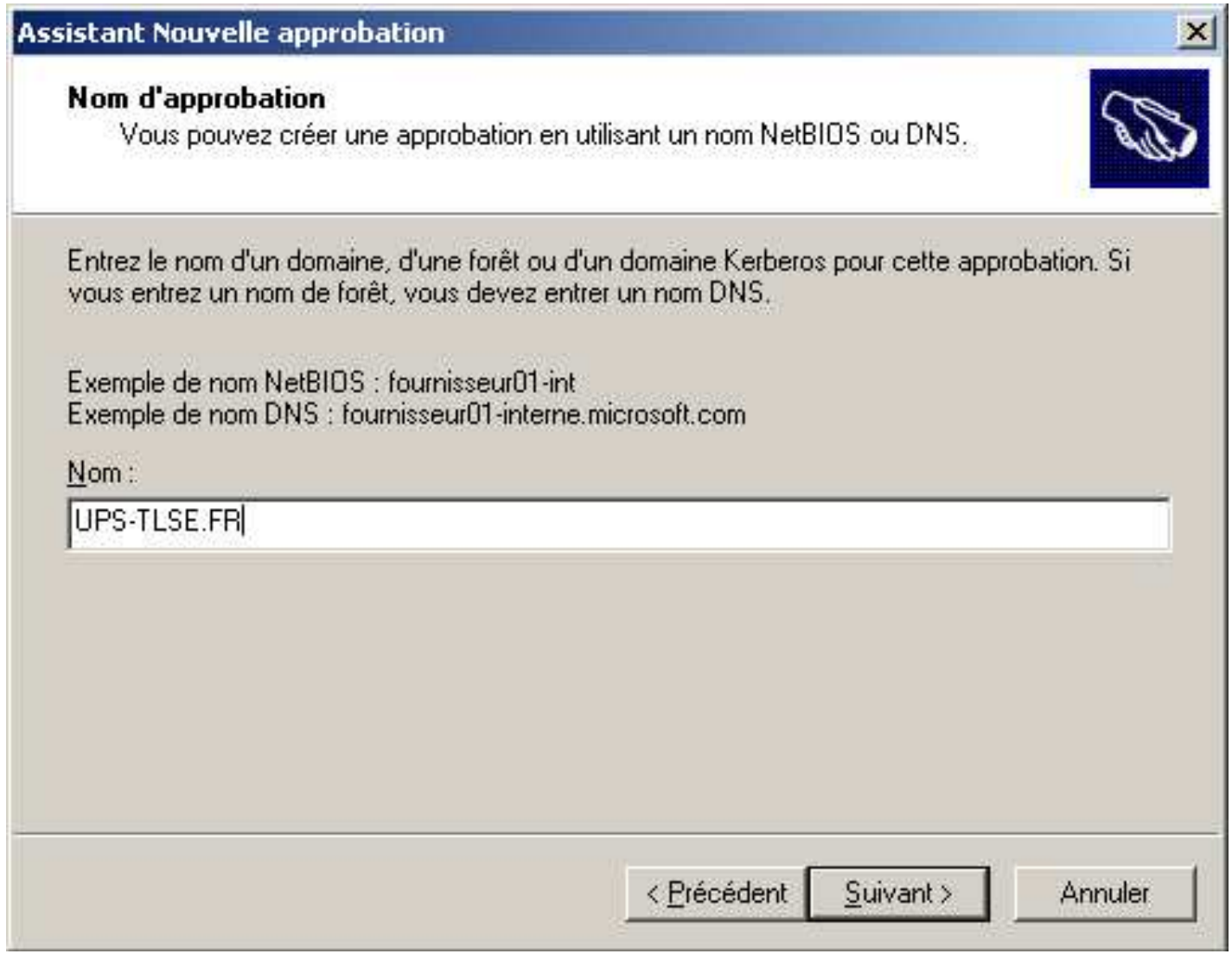
Approbation de domaines



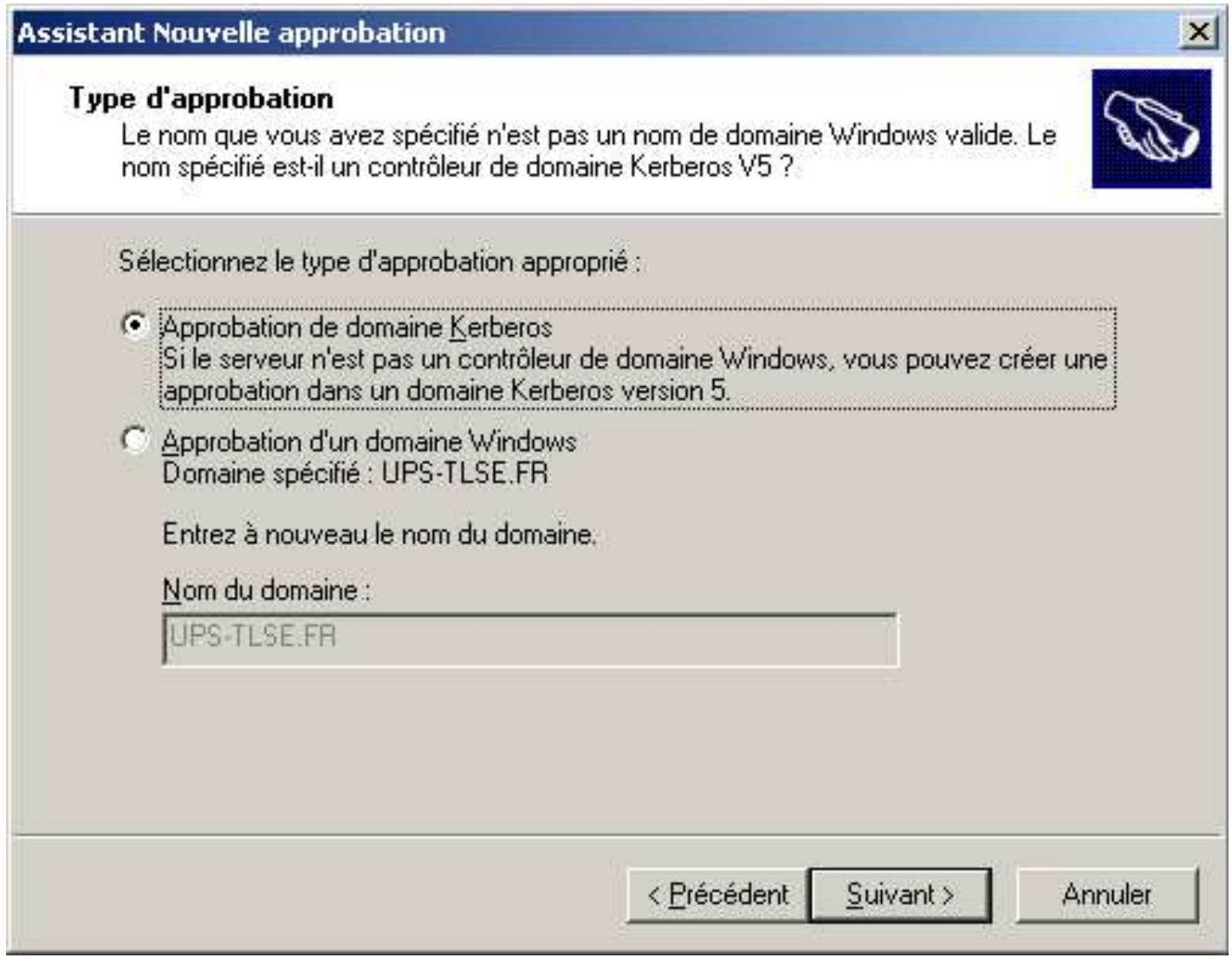
Approbation de domaines



Approbation de domaines



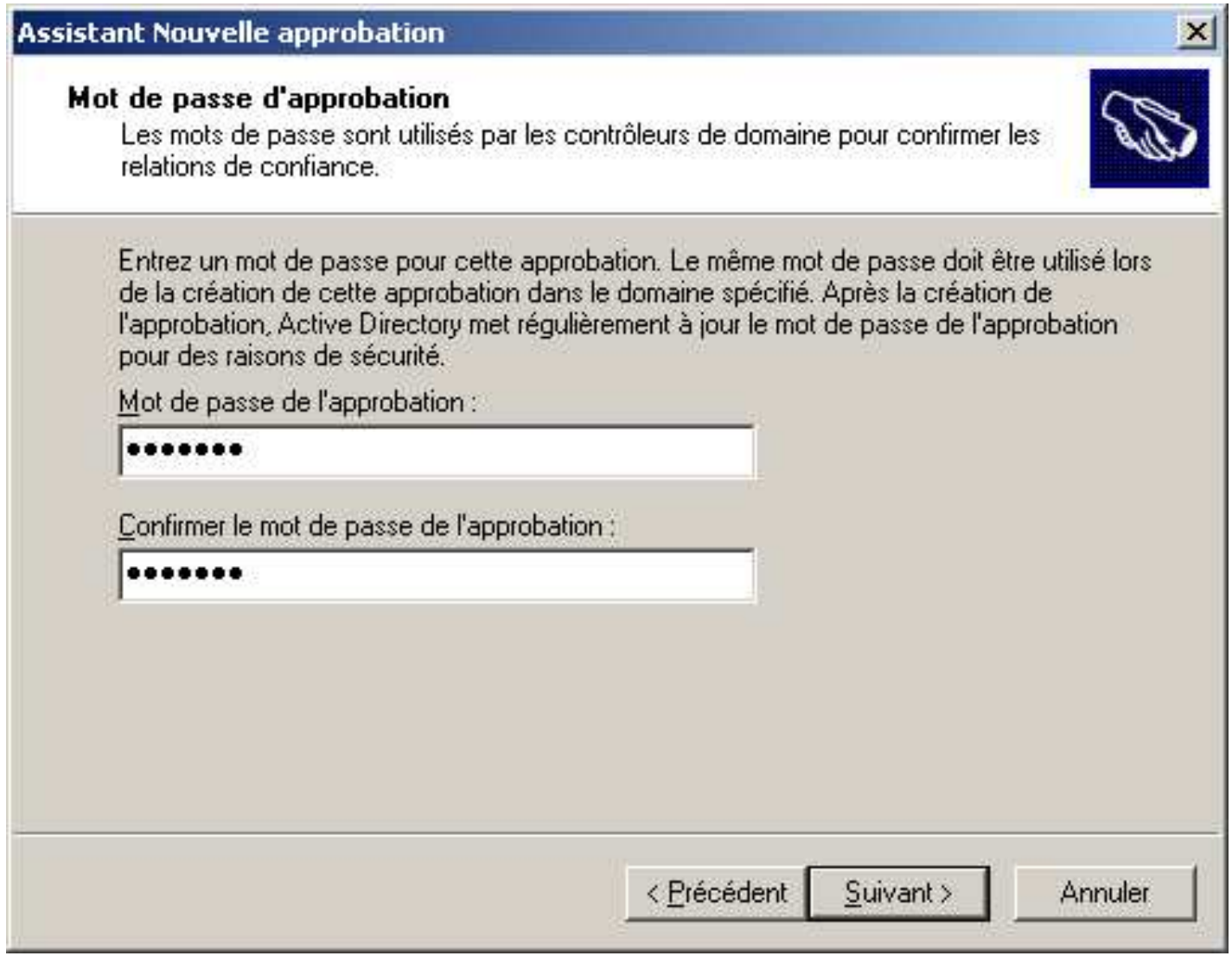
Approbation de domaines



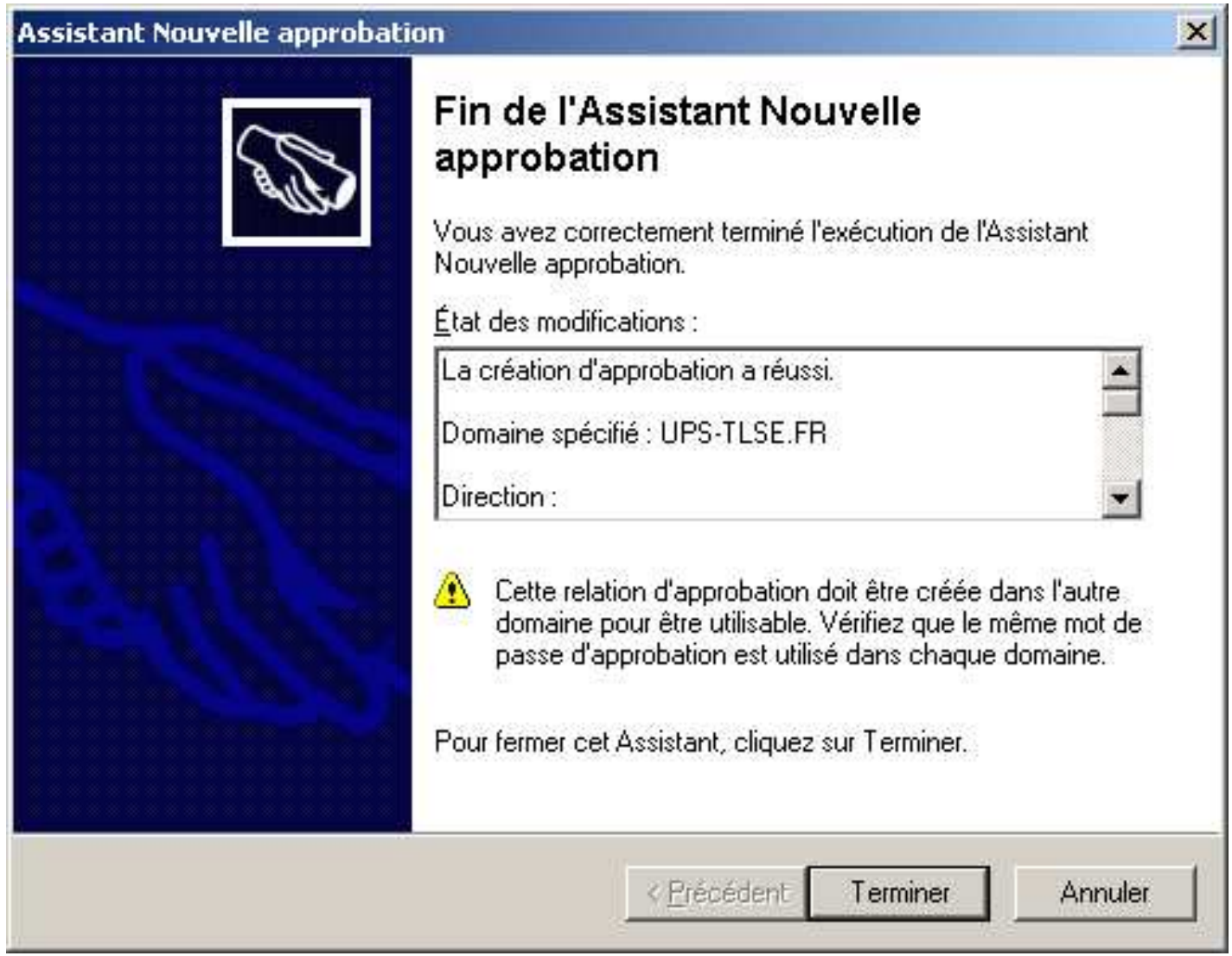
Approbation de domaines

Approbation de domaines

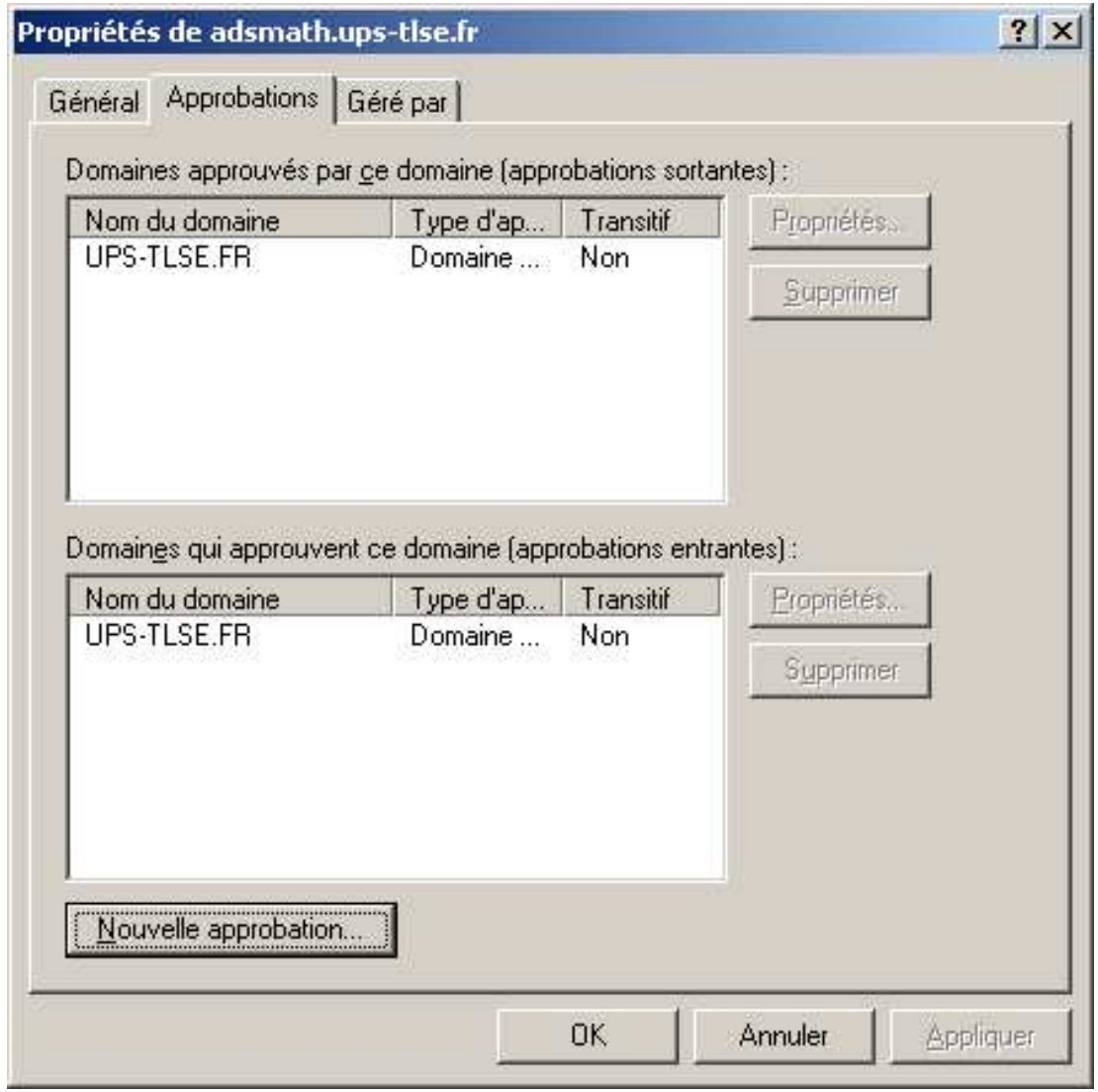
Approbation de domaines



Approbation de domaines

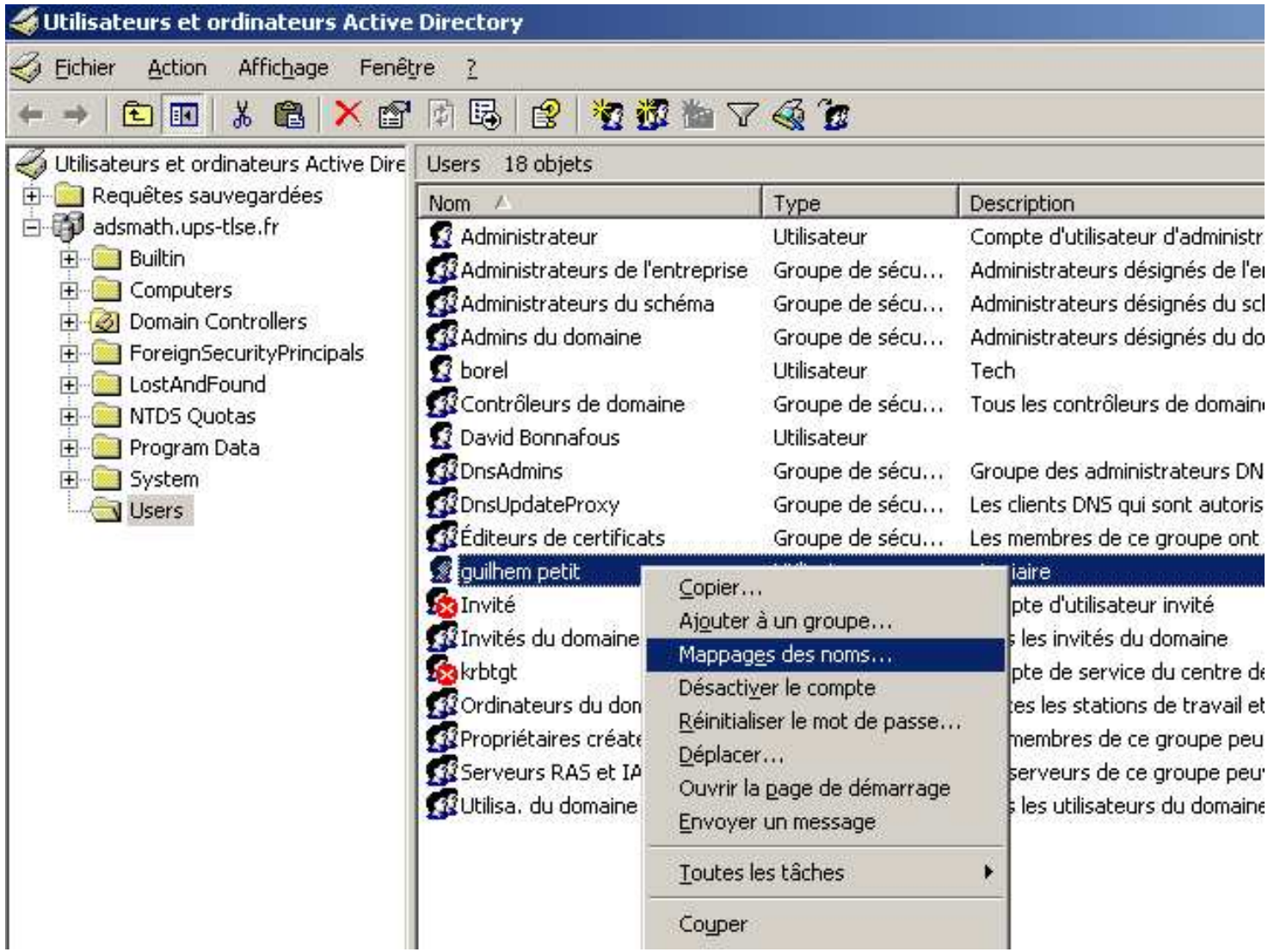


Approbation de domaines



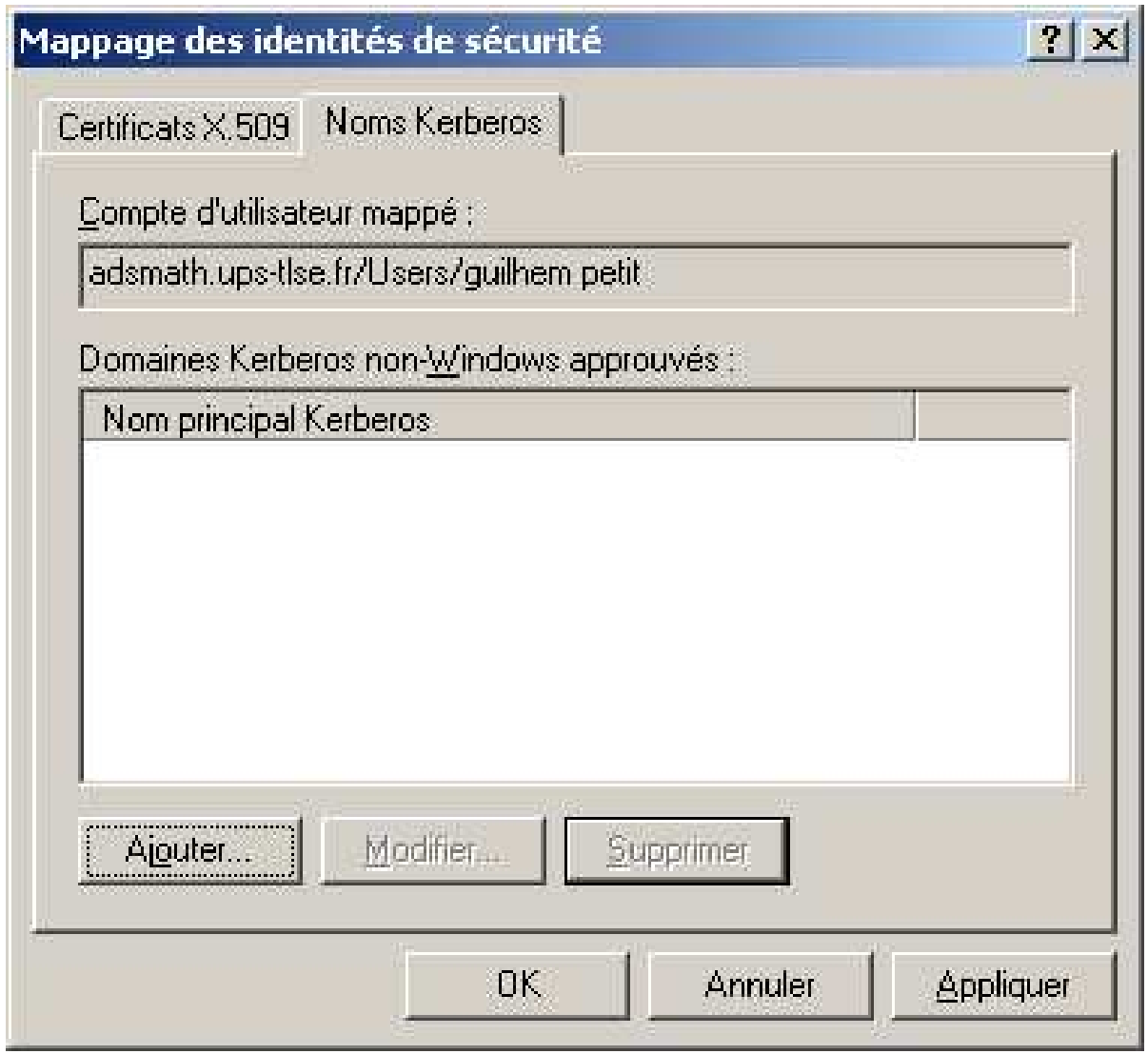
Approbation de domaines

mapping entre utilisateurs de l'AD et les principaux du KDC



Approbation de domaines

mapping entre utilisateurs de l'AD et les principaux du KDC

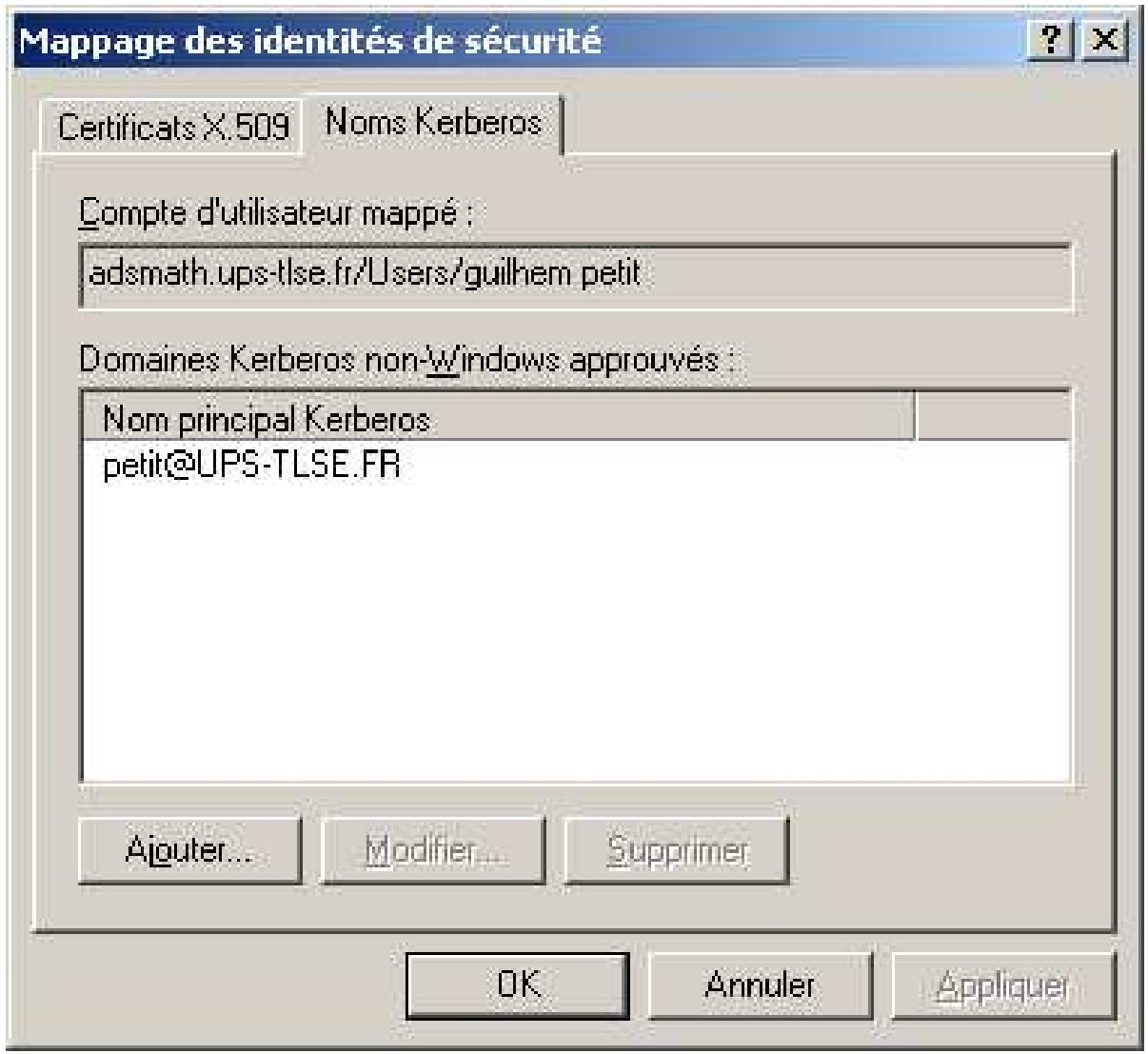


Approbation de domaines

mapping entre utilisateurs de l'AD et les principaux du KDC

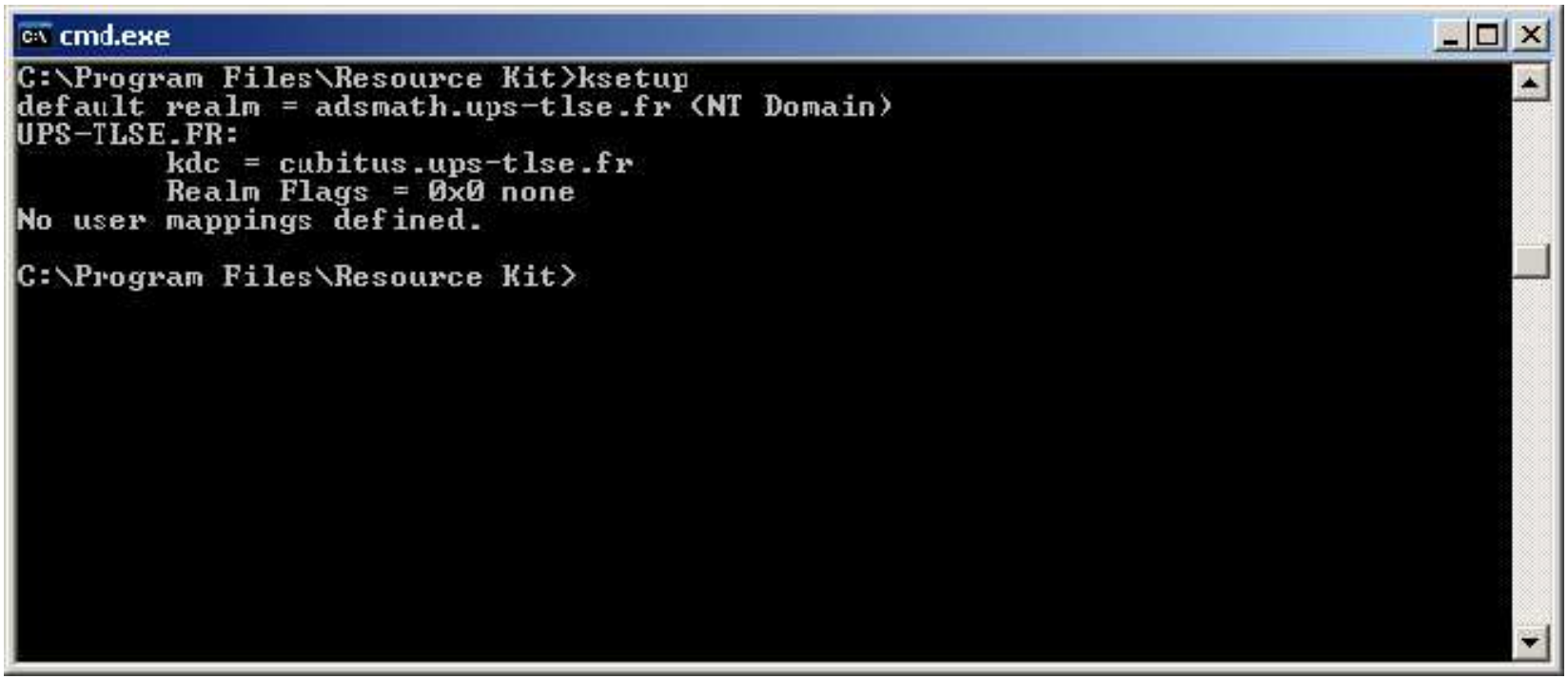
Approbation de domaines

mapping entre utilisateurs de l'AD et les principaux du KDC



Approbation de domaines

toutes les machines du domaine AD doivent connaître le royaume kerberos et les KDC



Difficultés et perspectives

- scripter la création d'un compte dans Active Directory avec les bons paramètres (mapping)
- faire fonctionner le changement de mot de passe
- invalider le mot de passe dans Active Directory
- tester le SSO avec ssh (putty) entre Windows et Linux
- Mac OS X
- Thunderbird, IMAP ?
- Firefox, Apache ?
- samba ?
- ...

Encore plus

- LDAP[1]
- IETF Working Group (krb-wg) actif
  http ://www.ietf.org/html.charters/krb-wg-charter.html

Encore plus

Références

[1] V. Le Poupon and V. Royer. Authentification forte d'un serveur LDAP par la méthode kerberos. Projet de fin d'étude, Institut National des Télécommunications, juin 2004.

Encore plus

- XDM, GDM,...

trademark

- Linux® is the registered trademark of Linux Torvalds in the U.S. and other countries.
- Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.
- NetBSD® is a registered trademark of The NetBSD Foundation.
- Mac OS X® is a registered trademark of Apple Computer.
- UNIX® is a registered trademark of The Open Group.

Bibliographie

[1]

Références

[1] Emmanuel le Chevoir. Étude de kerberos 5. Technical report, Hervé Schauer Consultants.