Kerberos, un vrai SSO ?

Revision : 1.7

david.bonnafous@math.ups-tlse.fr

www.math.univ-toulouse.fr/∼dbonnafo

Kerberos, un vrai SSO ?

- système d'authentification (pour l'identification : LDAP, NIS)
- utilisable dans beaucoup de configurations
- avec un petit effort on peut faire du SSO...

Plan de la présentation

- kerberos en bref
- utilisation : développement d'application
- utilisation : administration système
- kerberos unleashed : approbation de royaumes

Kerberos en bref

- système d'authentification pour des systèmes en réseau ouvert
- première apparition en 1988 [3]
- Kerberos 5, RFC 4120, juillet 2005
- mise à jour :
  - RFC 4537, Juin 2006
  - RFC 5021, août 2007
- groupe de travail de l'IETF, **krb-wg**
- beaucoup de doc : [1], [2]

Kerberos en bref : bibliographie

Références

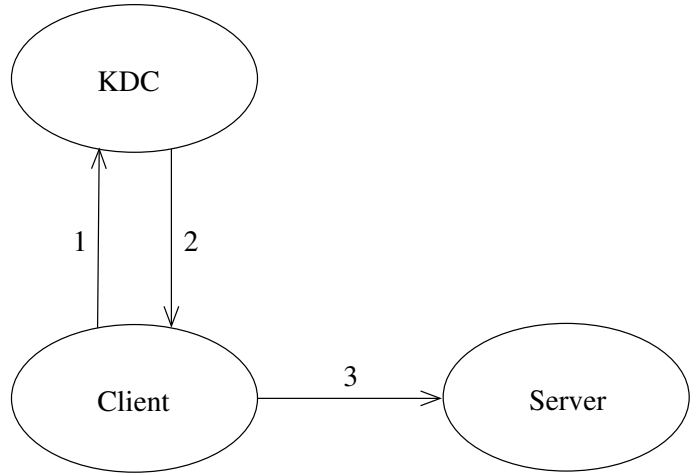
[1] Jason Garman. *Kerberos : The Definitive Guide*. O'Reilly, 2003.

[2] John T. Kohl, B. Clifford Neuman, and Theodore Y. Ts'o. The evolution of the kerberos authentication service. In IEEE Computer Society Press, editor, *Distributed Open Systems*, 1994.

[3] 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.

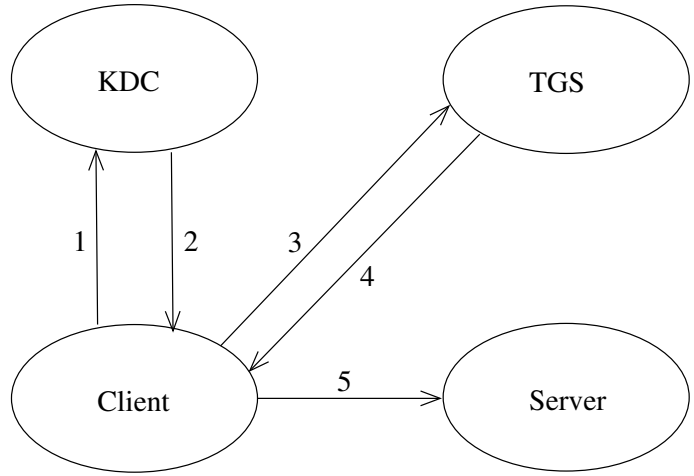
- http ://en.wikipedia.org/wiki/Kerberos_(protocol)
- http ://www.kerberos.isi.edu/

kerberos : ticket initial



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 : ticket de service



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

utilisation

point de vue du développeur

- SASL
- gssapi
- pam
- les implémentations

SASL

- Simple Authentication and Security Layer
- groupe de travail sasl de l'IETF, **sasl**
- négotiation du système d'authentification pour les applications client/serveur
- en particulier le mécanisme GSSAPI (kerberos V)

SASL

- API (incompatible) en c :
  - GNU SASL Library - Libgsasl
  - Cyrus SASL Library
  - dovecot SASL ?
- php, perl, java (jsr28)

SASL avec le mécanisme GSSAPI

- applications serveurs
  - sendmail
  - cyrus IMAP, dovecot
  - OpenLDAP
  - BEEP, librairies de développement d'application réseau
- applications clientes
  - Emacs Gnus (imtest de cyrus imap ou gsasl)
  - fetchmail
  - thunderbird

GSS API

interface de programmation générique pour la sécurité dans une application client/serveur

- authentification, intégrité, confidentialité
- RFC2743, Generic Security Service Application Program Interface Version 2, Update 1, janvier 2000
- RFC4121, The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism : Version 2, juillet 2005 ; RFC1964 juin 1996
- groupe de travail **kitten** de l'IETF, GSS-API next generation

GSS API

- GSS-API Programming Guide, Sun Microsystems
- http ://en.wikipedia.org/wiki/Generic_Security_Services_Application_Program_Interface

GSS API

- C, java, C#, perl
- heimdal, MIT
- GNU Generic Security Service Library (GSSLib)

GSS API

- application : mutt, Emacs Gnus, thunderbird
- firefox, openssh
- dovecot, apache mod_auth_kerb
- cups
- RPCSEC_GSS=RPC+GSSAPI : NFSv4, nfsv3
- xdm, gdm, kdm ?

SASL, mécanisme gssapi de SASL, GSS API

- le mécanisme gssapi de SASL = kerberos grâce à l'API de GSS-API
- 9 octobre 2007, draft, "Using GSS-API Mechanisms in SASL : The GS2 Mechanism Family"

PAM

Pluggable Authentication Modules

- http ://www.kernel.org/pub/linux/libs/pam/
- http ://sourceforge.net/projects/pam-krb5/

PAM et kerberos ?

avec les modules kerberos de PAM on authentifie l'utilisateur avec son mot de passe pas les tickets...

- application cliente = application serveur
- PAM n'est pas pour les applications client/serveur

kerberos : implémentations

- MIT
- heimdal
- shishi
- API incompatibles mais implémentations inter-opérables

kerberiser les applications

utilisation

point de vue de l'administrateur

- les applications
- Active Directory et linux : kerberos

les applications

- apache et les clients (IE, firefox)
- IMAP et les clients (outlook, thunderbird)
- ssh
- cups
- AFS, NFSv4 (RPCSEC_GSS)
- openLDAP (SASL), SOCKS (GSS-API, RFC1961), samba

cross realm authentication

- confiance mutuelle entre 2 royaumes Kerberos
- un ticket du royaume A est accepté dans le royaume B
- $\longrightarrow$ création de clès inter-domaines

Kerberos, UNIX et Windows [3] [2] [1]

Références

[1] Microsoft TechNet. Windows 2000 kerberos authentication.

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

[3] 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 solo, royaume Kerberos Linux

- 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.

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

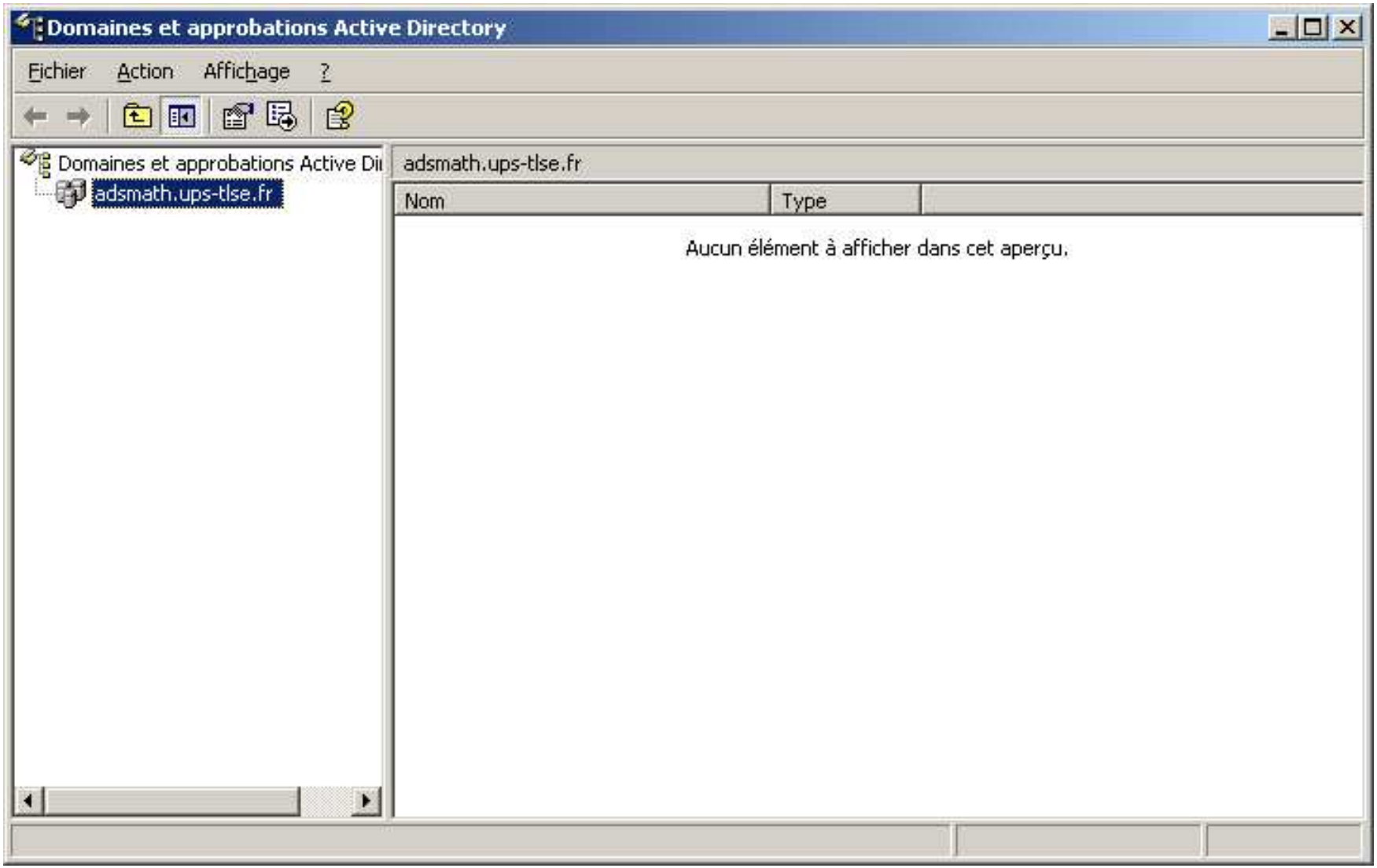
sur le contrôleur de domaine

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

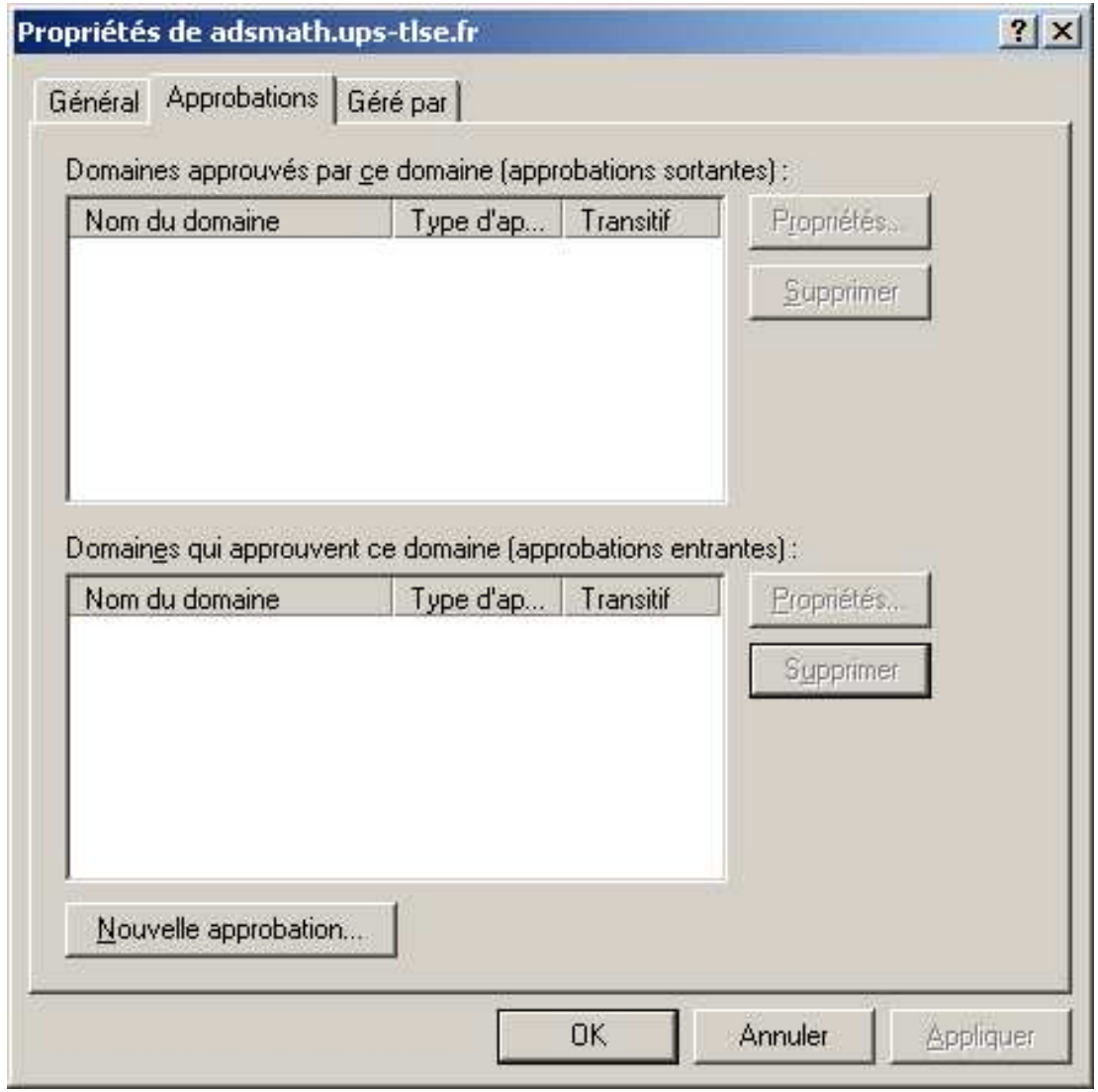
sur le KDC

- commande kadmin

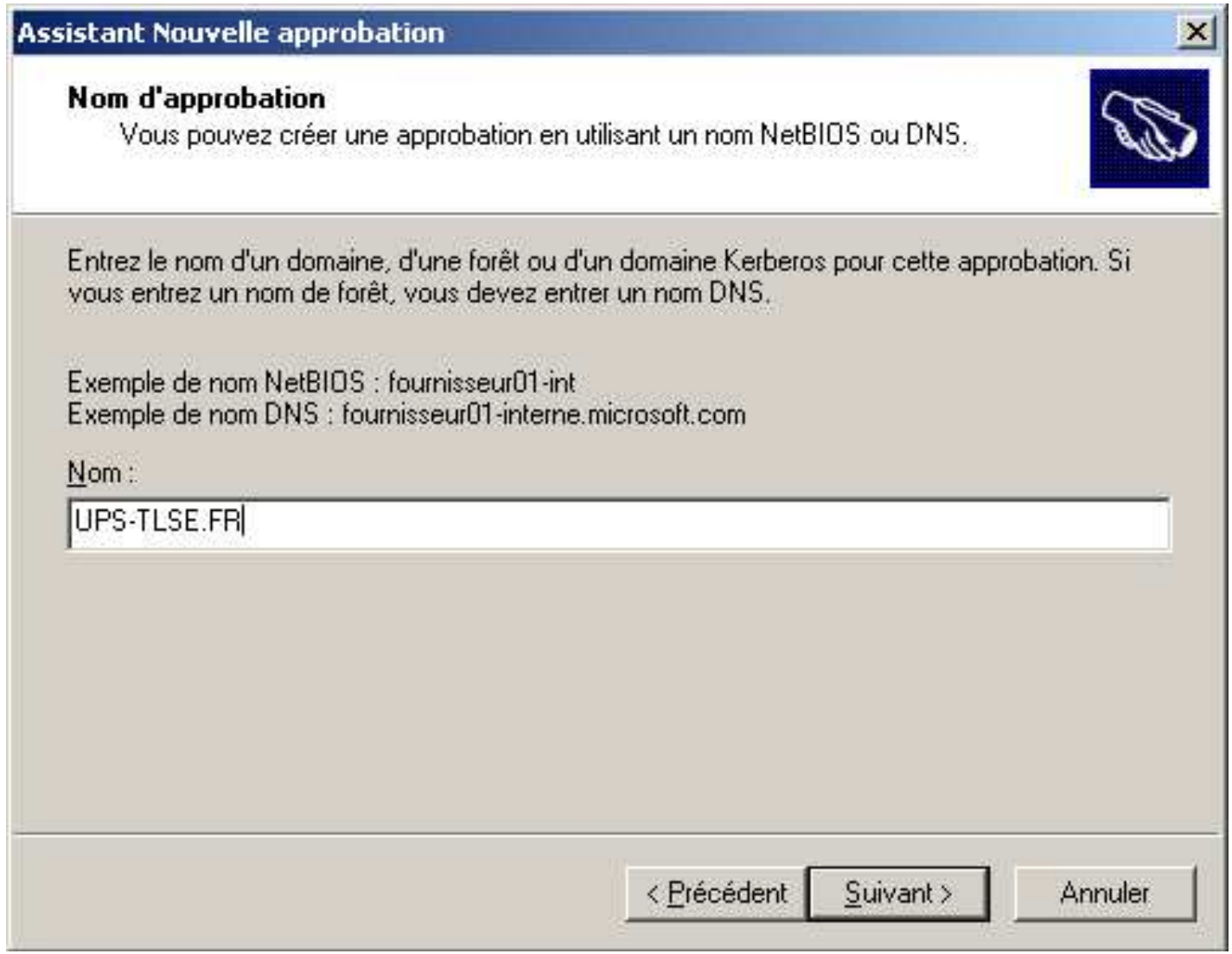
Approbation de domaines



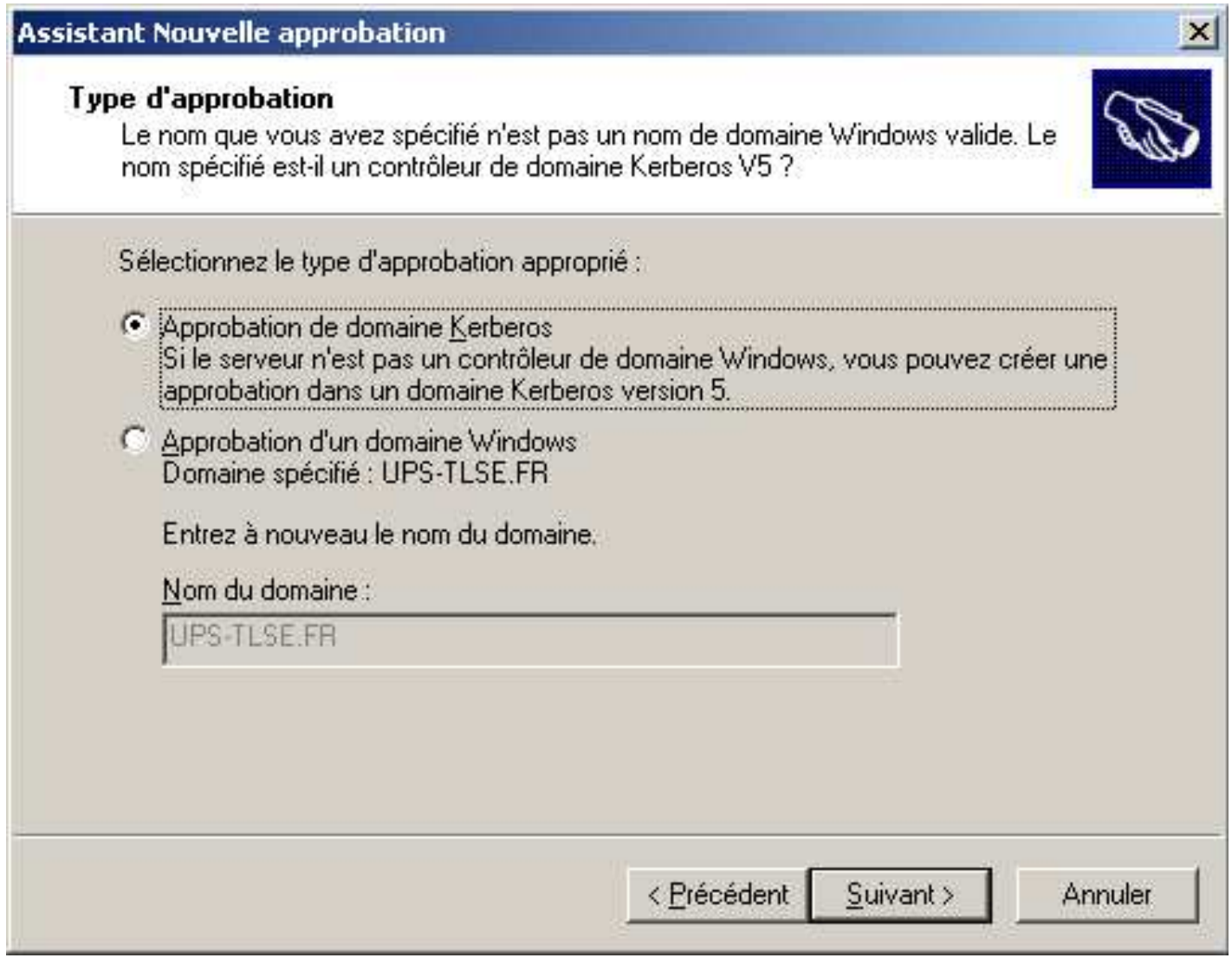
Approbation de domaines



Approbation de domaines



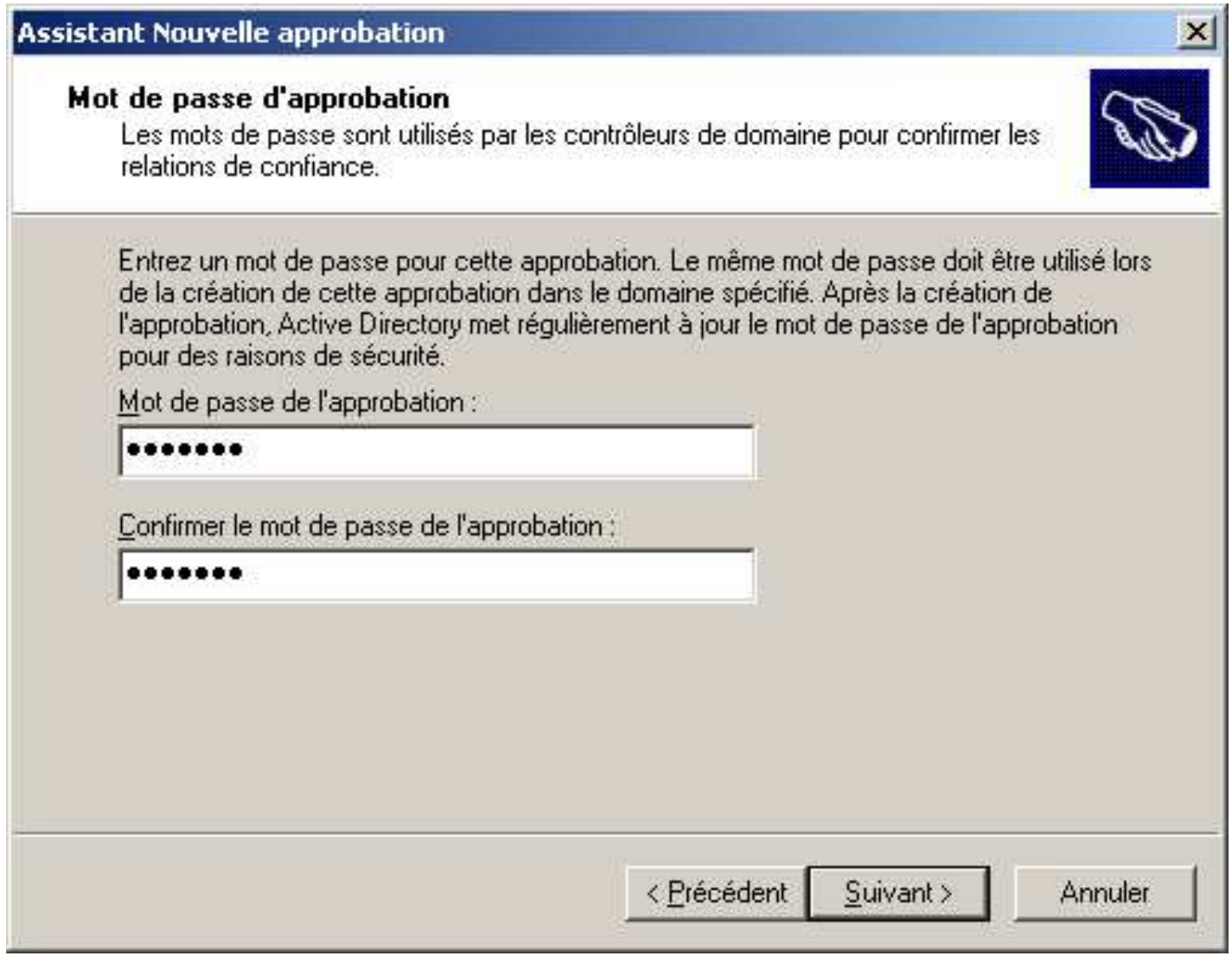
Approbation de domaines



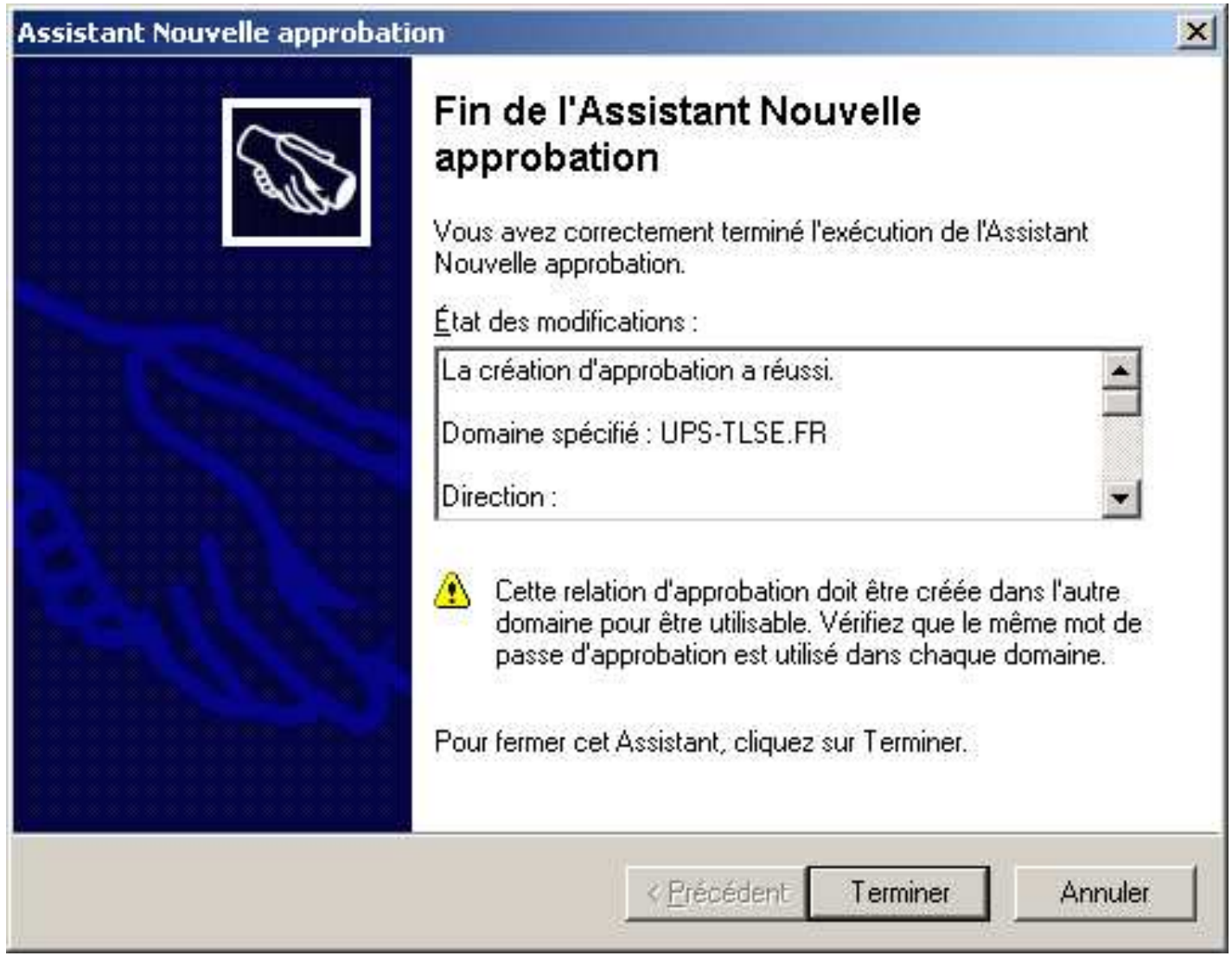
Approbation de domaines

Approbation de domaines

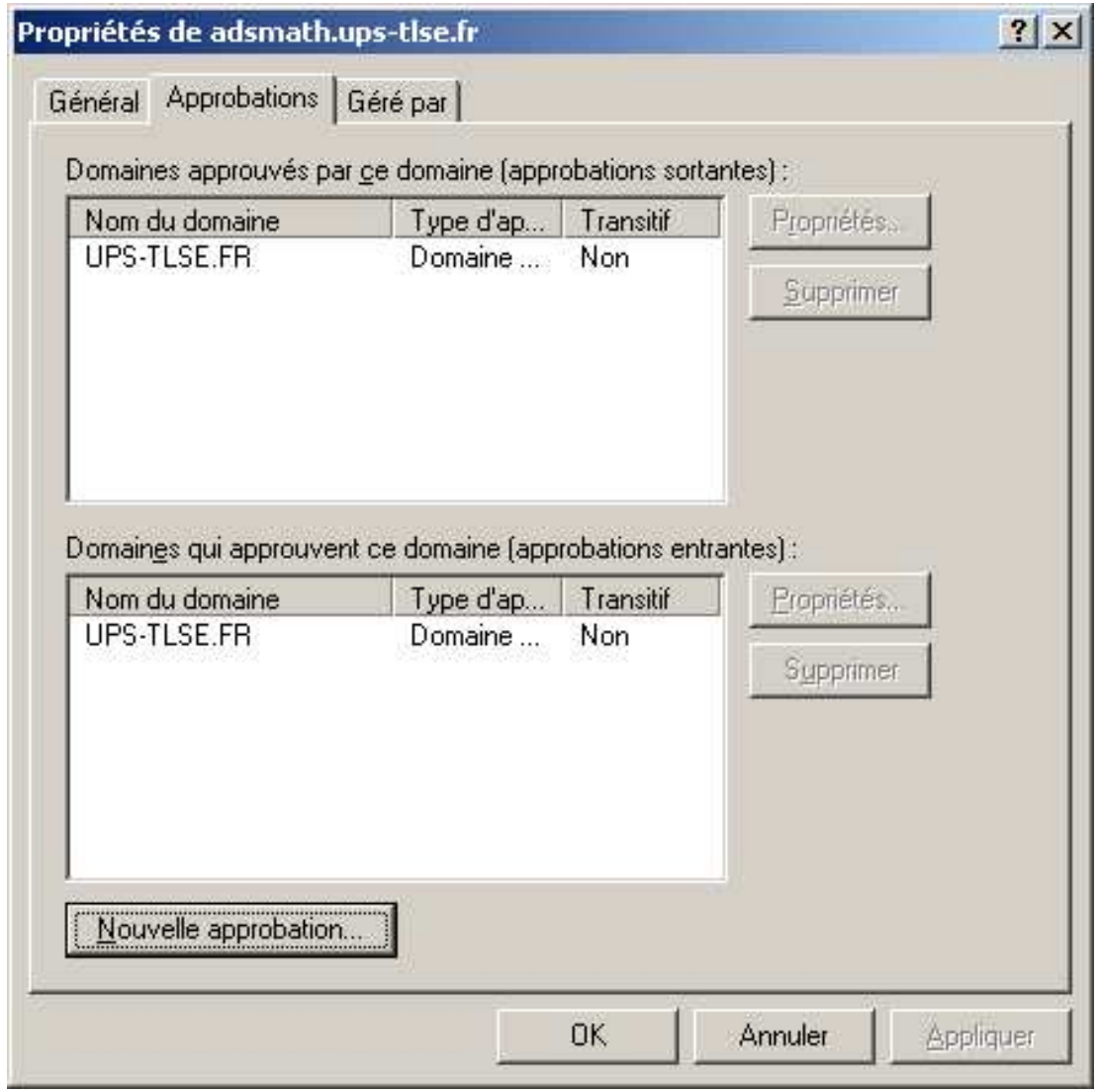
Approbation de domaines



Approbation de domaines

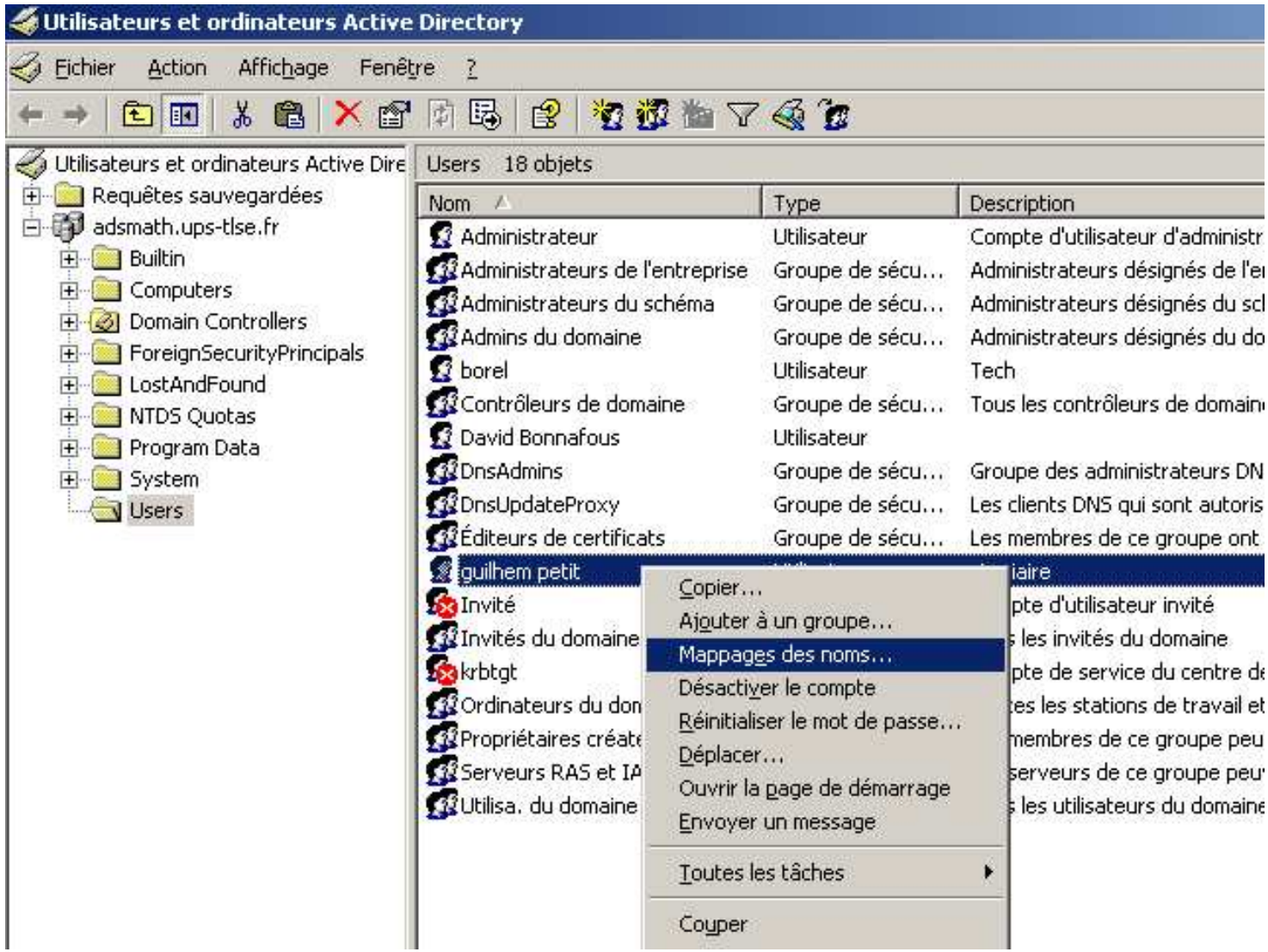


Approbation de domaines



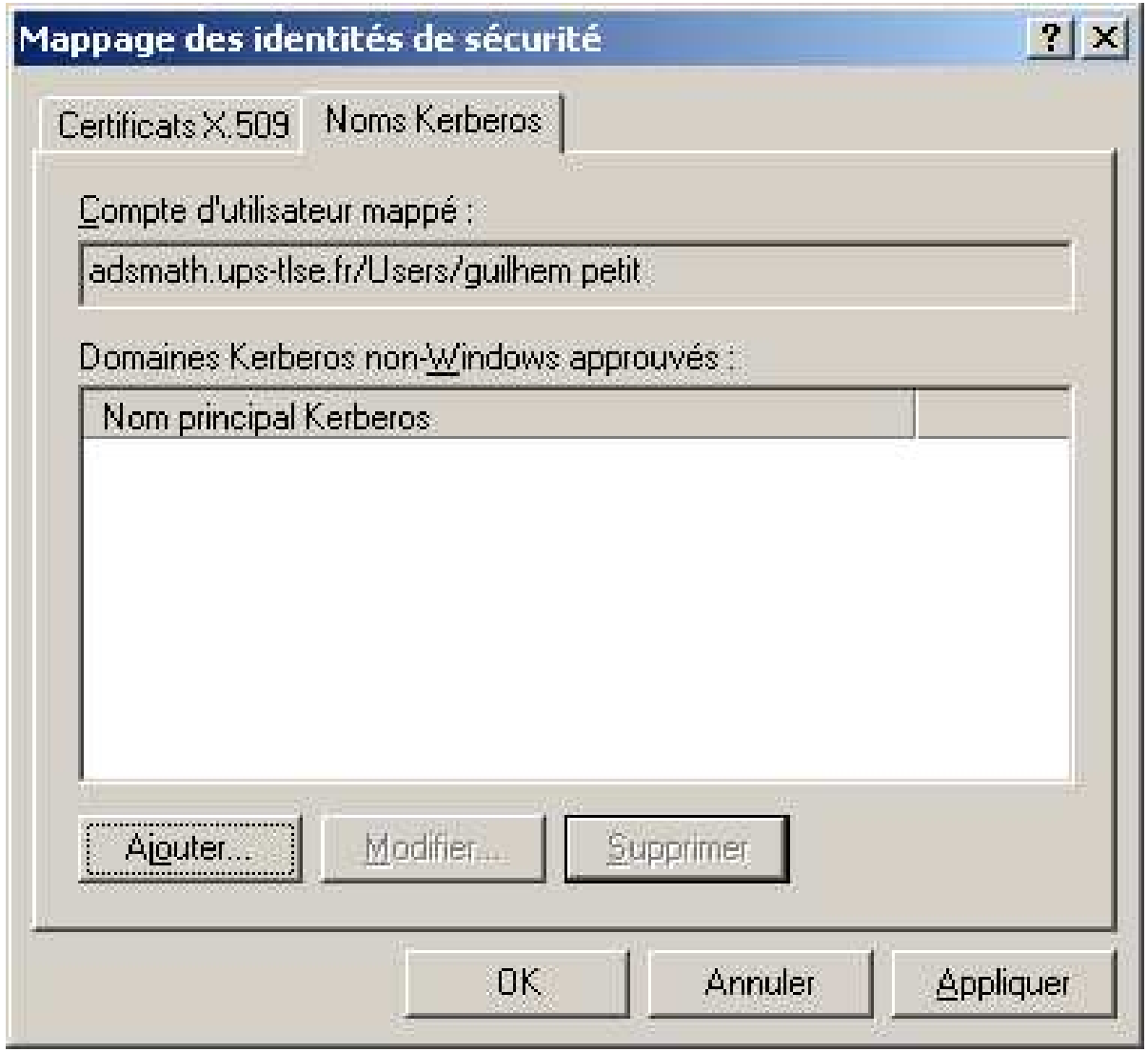
Approbation de domaines

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

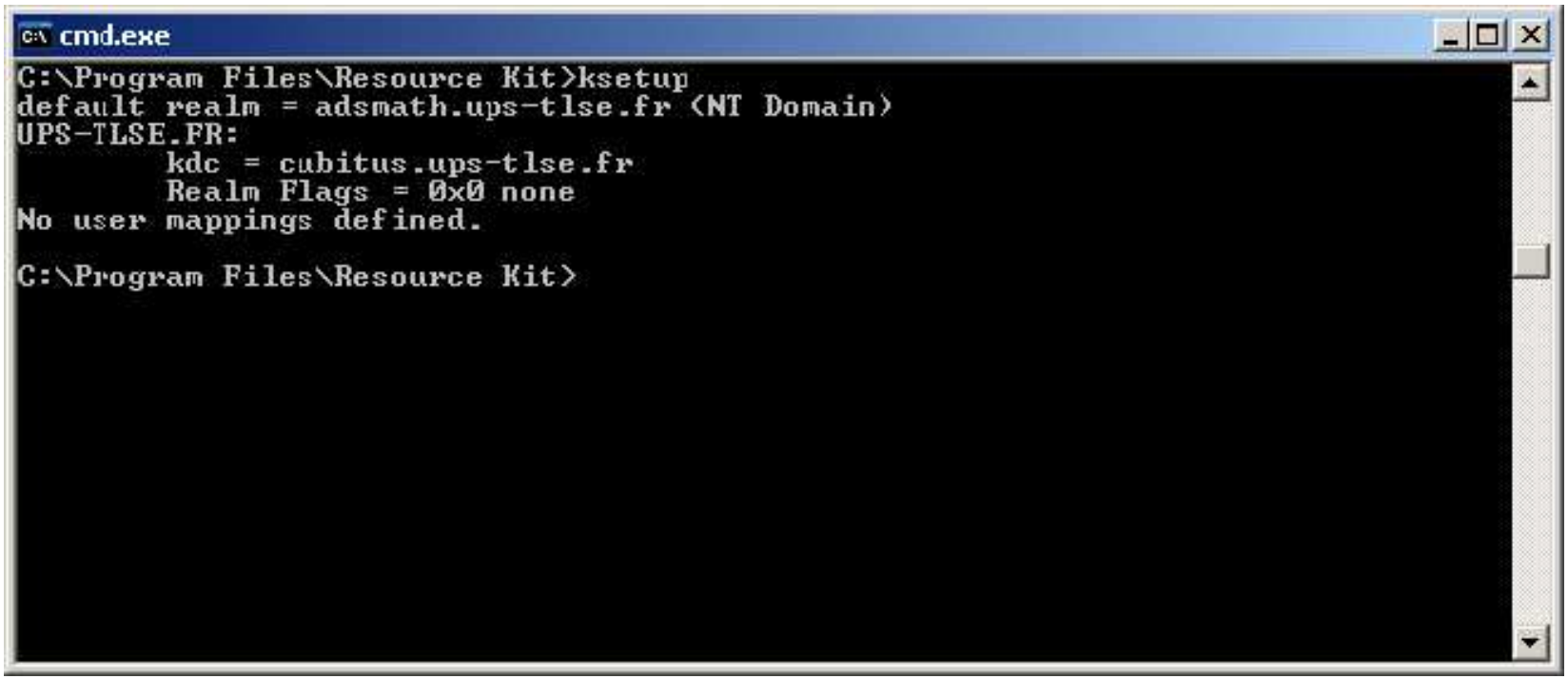
mapping entre utilisateurs de l'AD et les principaux du KDC

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
- écran de veille
- accès aux partages

Bibliographie

un article historique[1]

Références

[1] Roger Needham and Michael Schroeder. Using encryption for authentication in large networks of computers. *Communication of the ACM*, 21(12), 1978.