INFN Network & Computing

Workshop 2006
K5@Windows
Introduction to a global x-athent./author. model

Nunzio AMANZI, LNF - INFN
E-mail: Nunzio.Amanzi@lnf.infn.it
www: http://www.lnf.infn.it/~amanzi
Phone: +39 6 94 03 2607-8225

Subjects Menu

1 - OVERVIEWS

- Windows Kerberos V
- Infrastr. Model & Requirements

2 - LOCAL ENVIRONMENT TESTS

- Net/Dom Infrastructure
- Windows Tools
- K5 W-Authorization Process
- W-MIT K5 Host Single Sign-On
- AD K5 X-Authent./Authoriz.
- AD K5 Authoriz. Feedback
- K5 X-Auth. Tickets Flow

3 – GLOBAL CASE STUDY

- W-Domain Granting Scenario
- W-Domain Groups Model
- AD LDAP Names Space Layout
- AD LDAP NS Implementation
- W-Forest Trusts Tips
- Mixed Realms Trusts Tests

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

1 - Overviews

Windows Kerberos V

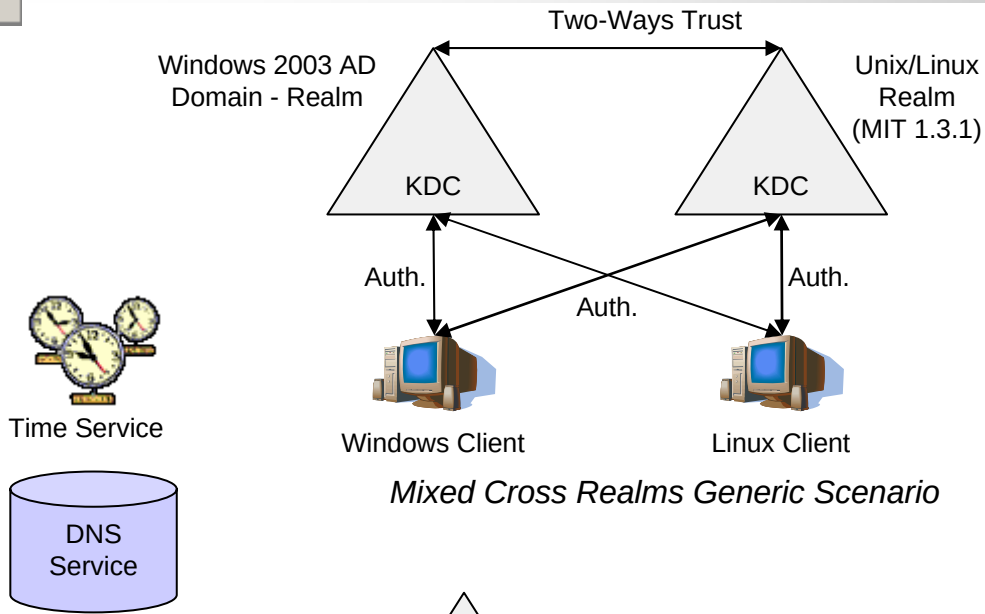
PERCHE' KERBEROS V

- Un Windows DC (2000 o sup.) implementa il KDC come servizio di dominio:
  - l'implementazione e' basata sulla RFC 1510
  - esporta l'Authentication Service (AS)
  - esporta il Ticket Granting Service (TGS)
  - utilizza AD DB come Kerberos Account DB
  - i servizi sono eseguiti nel process-space del LSA
- Un dominio di AD definisce un Kerberos V Realm
- Nei Wclient (2000/XP) aggiunti al WDom (2000/2003) K5 e' abilitato per default
- I sistemi unix/linux possono autenticarsi verso un KDC Windows mediante kinit
- I client windows possono utilizzare KDC unix/linux per il login in single sign-on

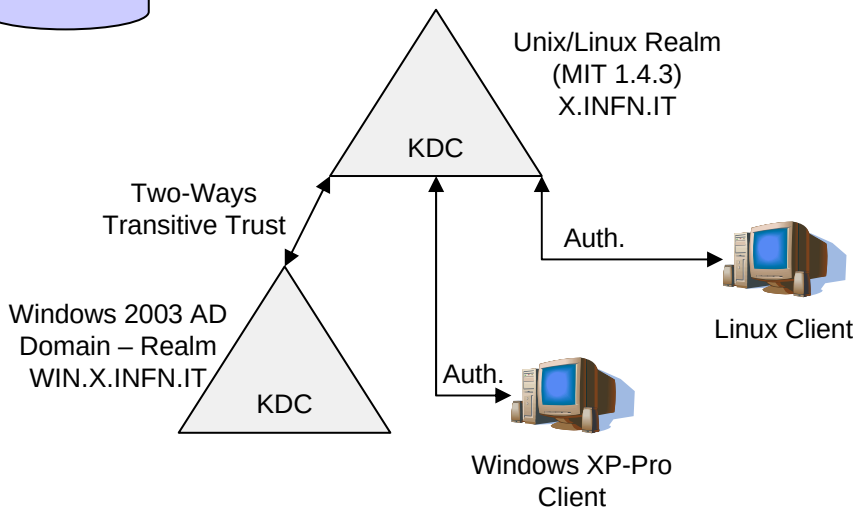
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

1 - Overviews

Infrastructure Model and Requirements



Mixed Cross Realms Generic Scenario



Local Implementation Scenario

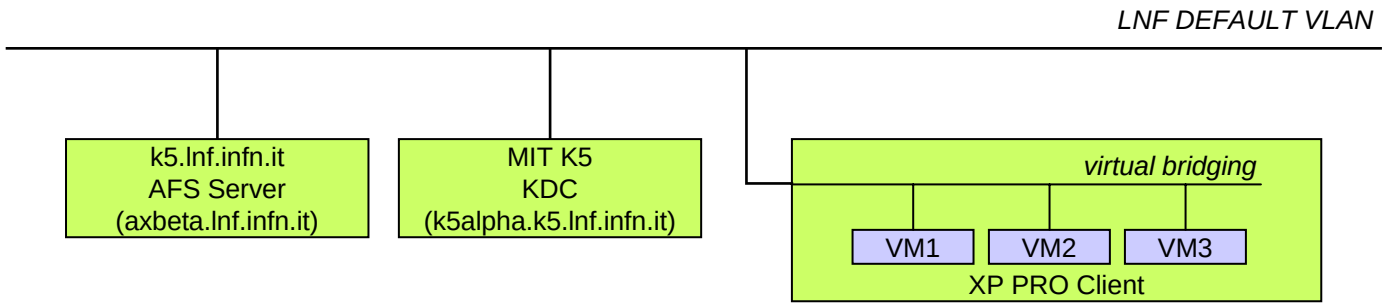
MODELLO LOCALE CONSIGLIATO

- Dominio Windows 2003 come sottodominio DNS di X.INFN.IT
- WIN.X.INFN.IT servito in modo autoritativo da Windows
- Unico provider ntp per la sincronizzazione dell'orario servito da Unix/Linux
- MIT Kerberos 1.4.3 o sup.
- Trust bidirezionale e transitivo
- Client Windows XP – Pro SP1 o sup.
- Unix/Linux Realm come regno di autenticazione in single sign-on

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

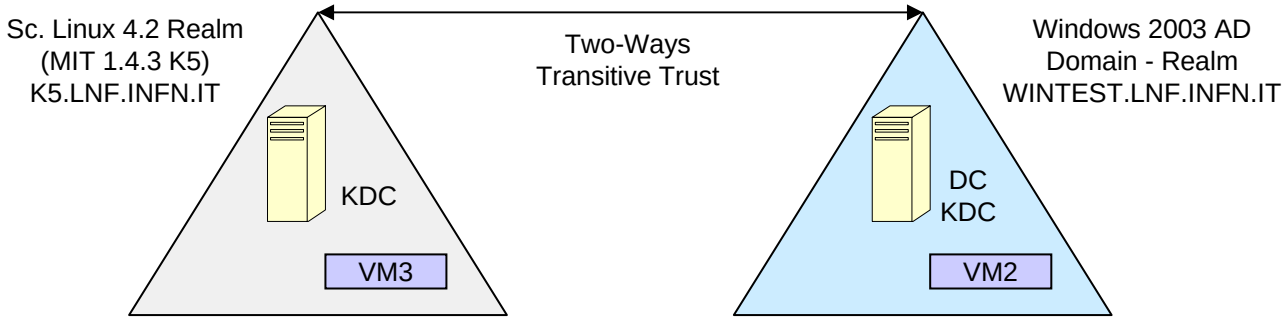
Networking/Domains Infrastructure



VM1 (winvrtsrv.wintest.lnf.infn.it), Windows 2003 Server: DC, KDC, DNS Server Autoritativo

VM2 (pcvrttest.wintest.lnf.infn.it), Windows Xp-Pro SP1: Windows Domain Client

VM3 (pcvrttest2.k5.lnf.infn.it), Windows Xp-Pro SP1: Windows MIT K5 Host



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

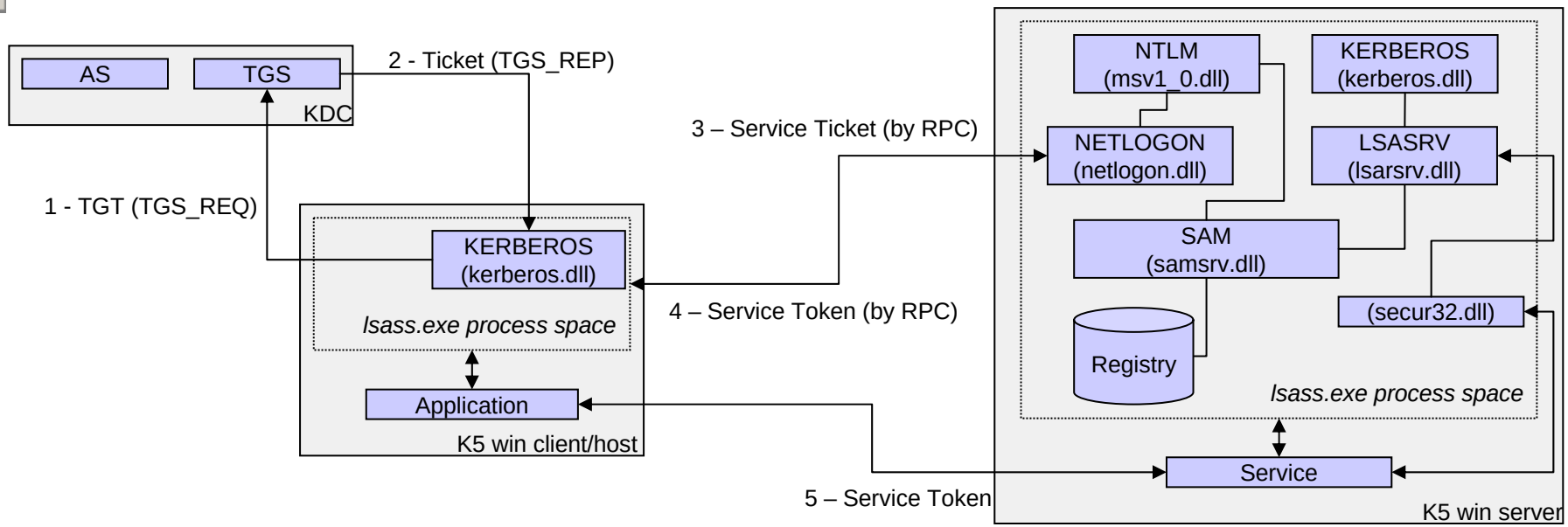
Windows Tools

Dsa.msc	Active Directory Users and Computers	Gestione utenti e GPO
Domain.msc	Active Directory Domains & Trusts	Gestione relazioni di trusts
Adsiedit.msc	ADSI Editor	Manager classi ADSI (W – Supp. Tools)
Schmmgmt.msc	Active Directory Schema	Manager metadata (schmmgmt.dll)
Regedit.exe	Registry Editor	Parametri kerberos e logging
Netdom.exe	Windows Domain Manager	Domain/Trust manager
Ksetup.exe	Kerberos realms setup command line tool	W – Supp. Tools
Ktpass.exe	Kerberos keytab setup command line tool	W – Supp. Tools
Kerbtray.exe	Kerberos tickets GUI tool	W2003 Res. Kit Tools
Kilst.exe	Kerberos tickets command line tool	W2003 Res. Kit Tools
Eventvwr.msc	Event Viewer	Feedback eventi K5
Netmon.exe	Network monitor	W2003 Standard Tool
Ldp.exe	Ldap support GUI tool	Manager LDAP (W – Supp. Tools)
.NET Framework 1.1	Development Libraries	Microsoft Downloads

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

K5 W-Authorization Process



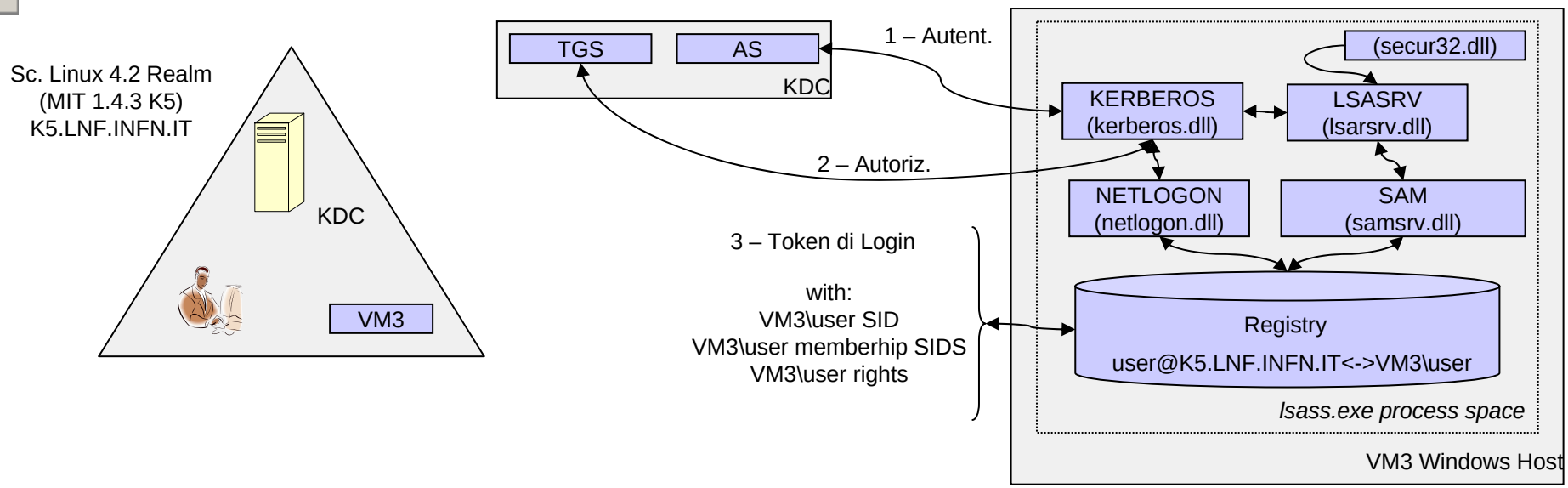
ACCESSO KERBERIZZATO AL SERVER MEMBRO DI DOMINIO

- il client invia al server un ticket di servizio
- il server negozia il ticket e restituisce al client un token per l'accesso al servizio
- il token contiene il SID dell'utente, dei gruppi di appartenenza (locali) e l'elenco dei diritti
- l'applicazione espone successivamente il token per l'intera sessione
- solo il ticket rilasciato da WKDC contengono informazioni di autorizzazione per l'utente autorizzato (PAC: Privilege Attribute Certificate)
- Per i ticket rilasciati da KDC non windows, la LSA Windows competente (nel DC o nel Server) determina le informazioni di protezione dell'utente mediante *mapping dei nomi*

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

Windows MIT K5 Host Single Sign-On



LA LSA DEL CLIENT RILASCIA LE INFORMAZIONI AUTORIZZAZIONE PER L'UTENTE

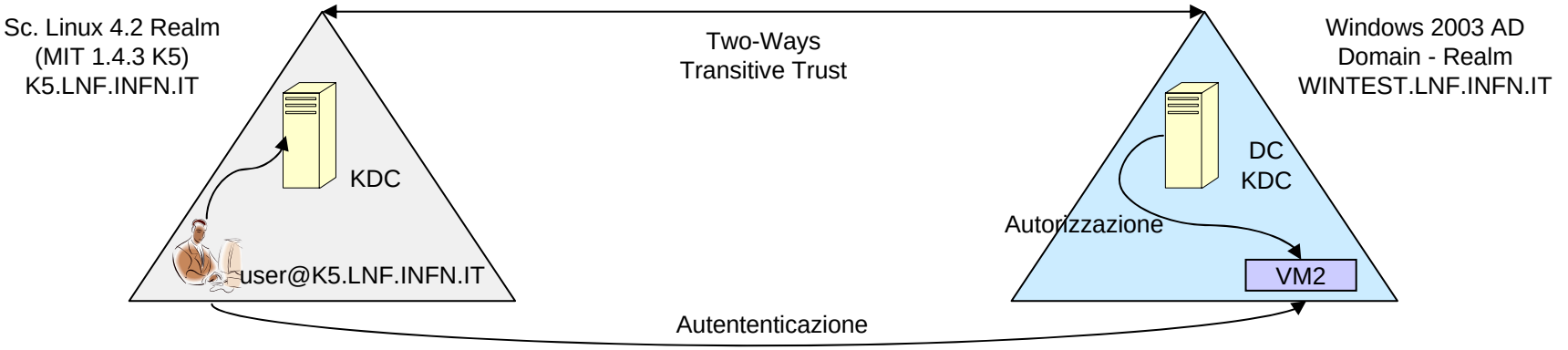
- VM3 e' un host windows membro di K5.LNF.INFN.IT (linux)
- Nel regno e' definito l'account utente K5 user@K5.LNF.INFN.IT
- In VM3 e' definito l'utente locale WM3\user
- VM3\user ha i privilegi per il login interattivo
- In VM3 e' definito il mapping user@K5.LNF.INFN.IT <-> VM3\user
- Quando l'utente si autentica in MIT K5 con le credenziali di user@K5.LNF.INFN.IT accede a WM3 in single sign-on con i privilegi dell'utente locale associato

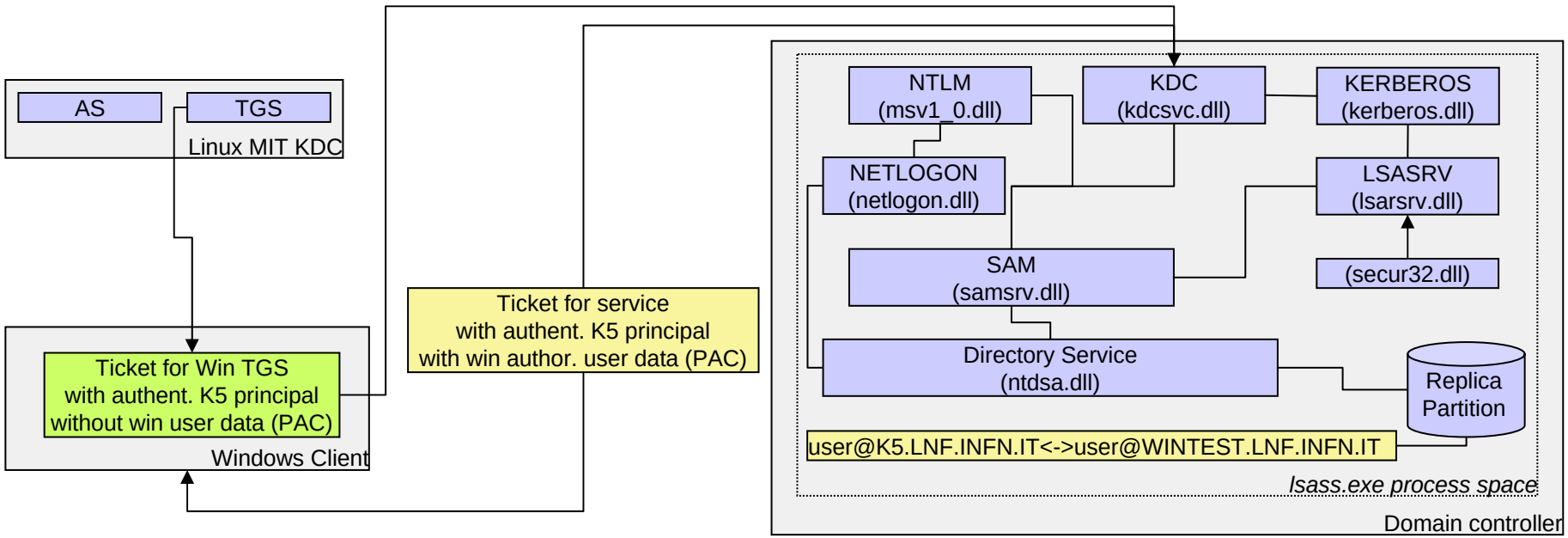
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

AD K5 X-Authent./Authoriz.

LA LSA DEL WDC (TGS) RILASCIA LE INFORMAZIONI DI AUTORIZZAZIONE DELL'UTENTE

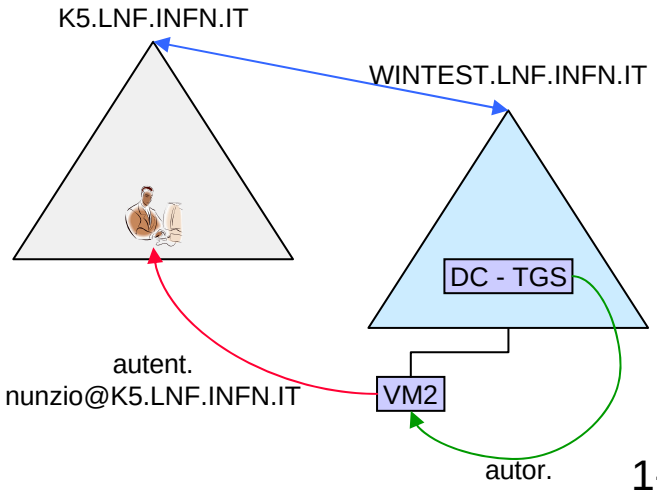




Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

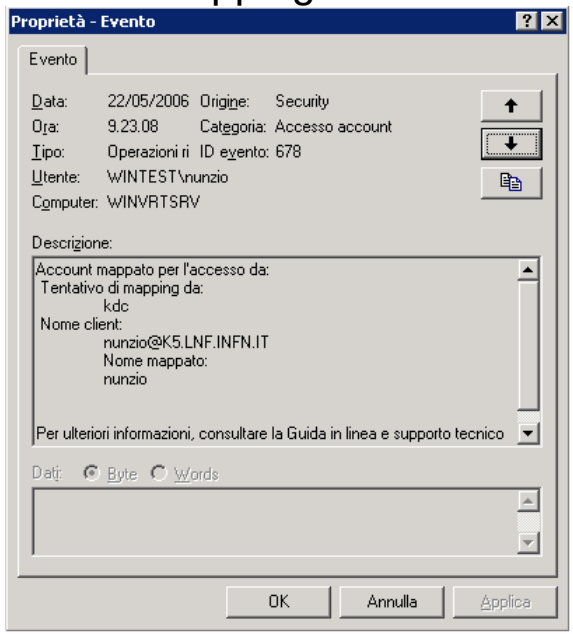
AD K5 Authorization Feedback



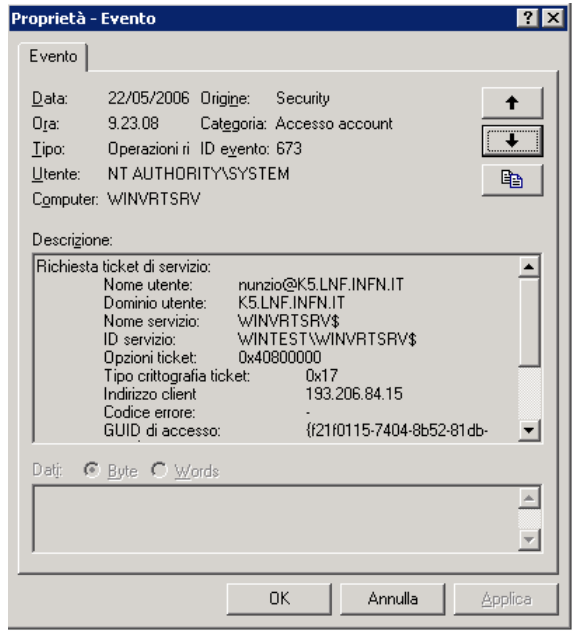
ABILITAZIONE AUDIT EVENTI DI PROTEZIONE MEDIANTE GPO DI DOMINIO

- Eventi di accesso account, relativi a tutte i processi di autenticazione/autorizzazione da parte del DC-KDC
- Eventi di accesso, relativi alle singole sessioni

1- user mapping



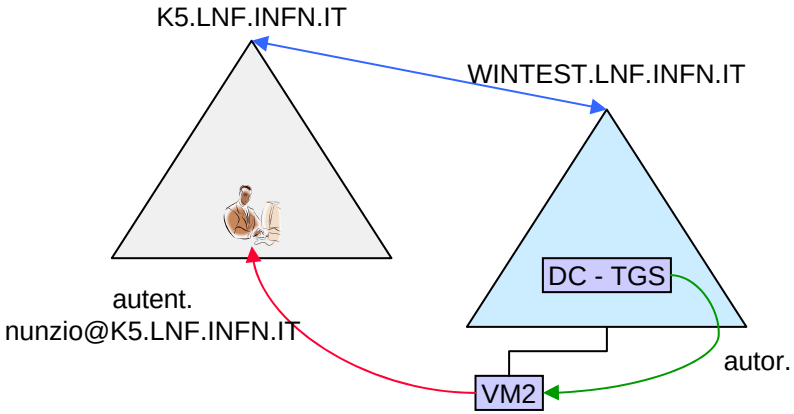
2 – rilascio service ticket

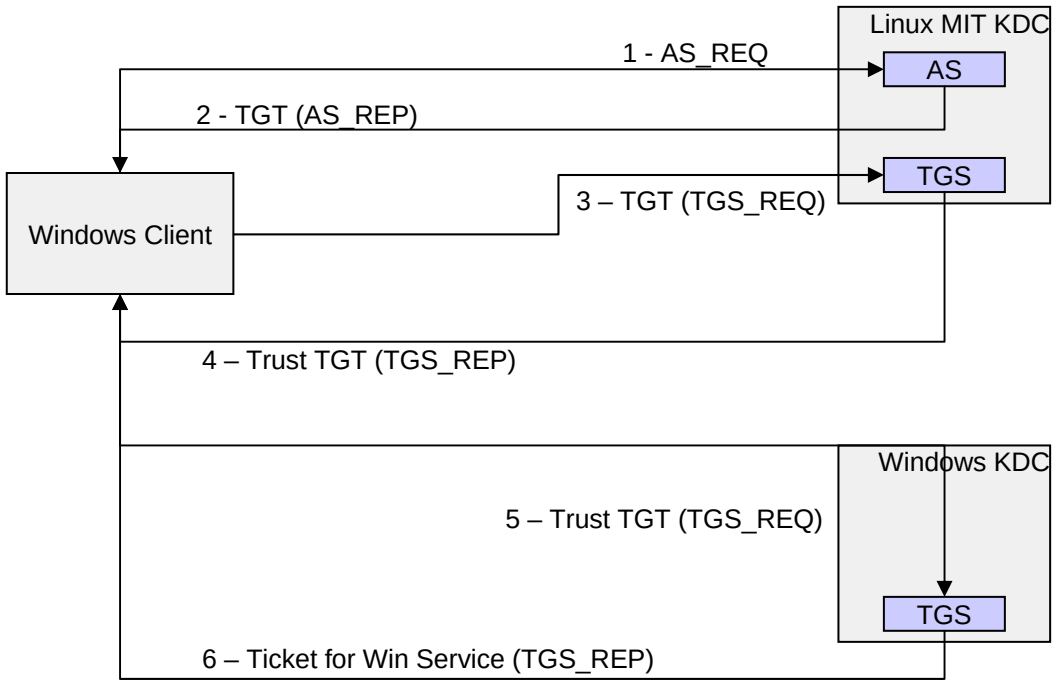


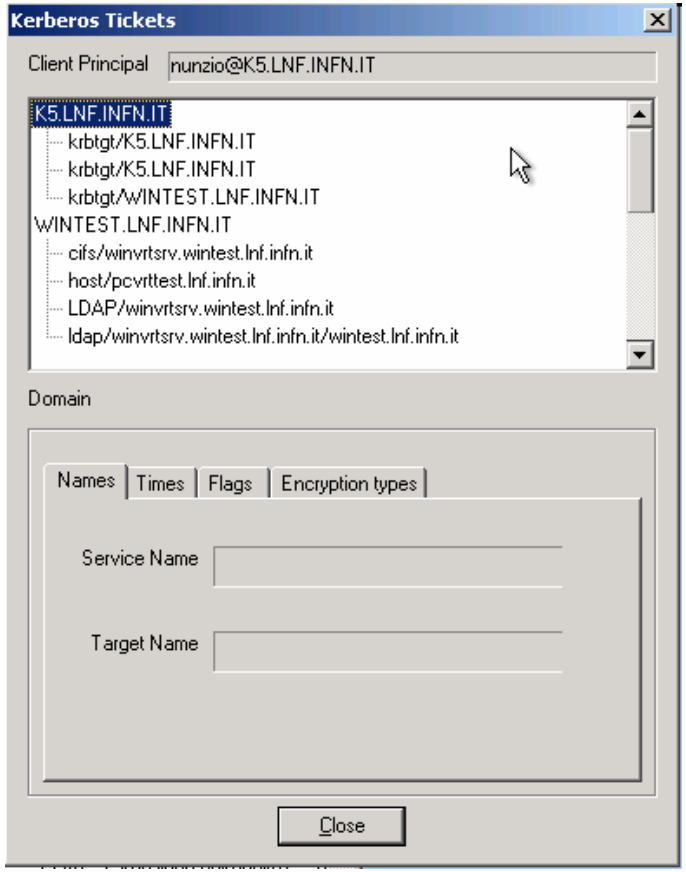
Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

2 - Local Environment Tests

K5 X-Auth. Tickets Flow







Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - Global Case Study

W-Domain Granting Scenario

PRESUPPOSTI/ASPETTI FUNZIONALI PER L'ACCESSO AI SERVIZI WINDOWS IN X-AUTH.

- L'utente e' autetenticato nel realm MIT K5 che definisce lo user account
- L'utente e' autorizzato dal dominio windows che esporta il servizio
- L'accesso ai servizi windows e' disciplinato in base ad un token relativo all'account utente definito in AD (trusting) e non in base al realm di autenticazione
- Non e' necessario conoscere le credenziali dell'account trusting in AD
- L'account trusting di AD e' sottoposto all'applicazione delle GPO
- Nelle sessioni di login interattivo e' utilizzato il profilo utente dell'account trusting

PROCEDURE IMPLEMENTATIVE

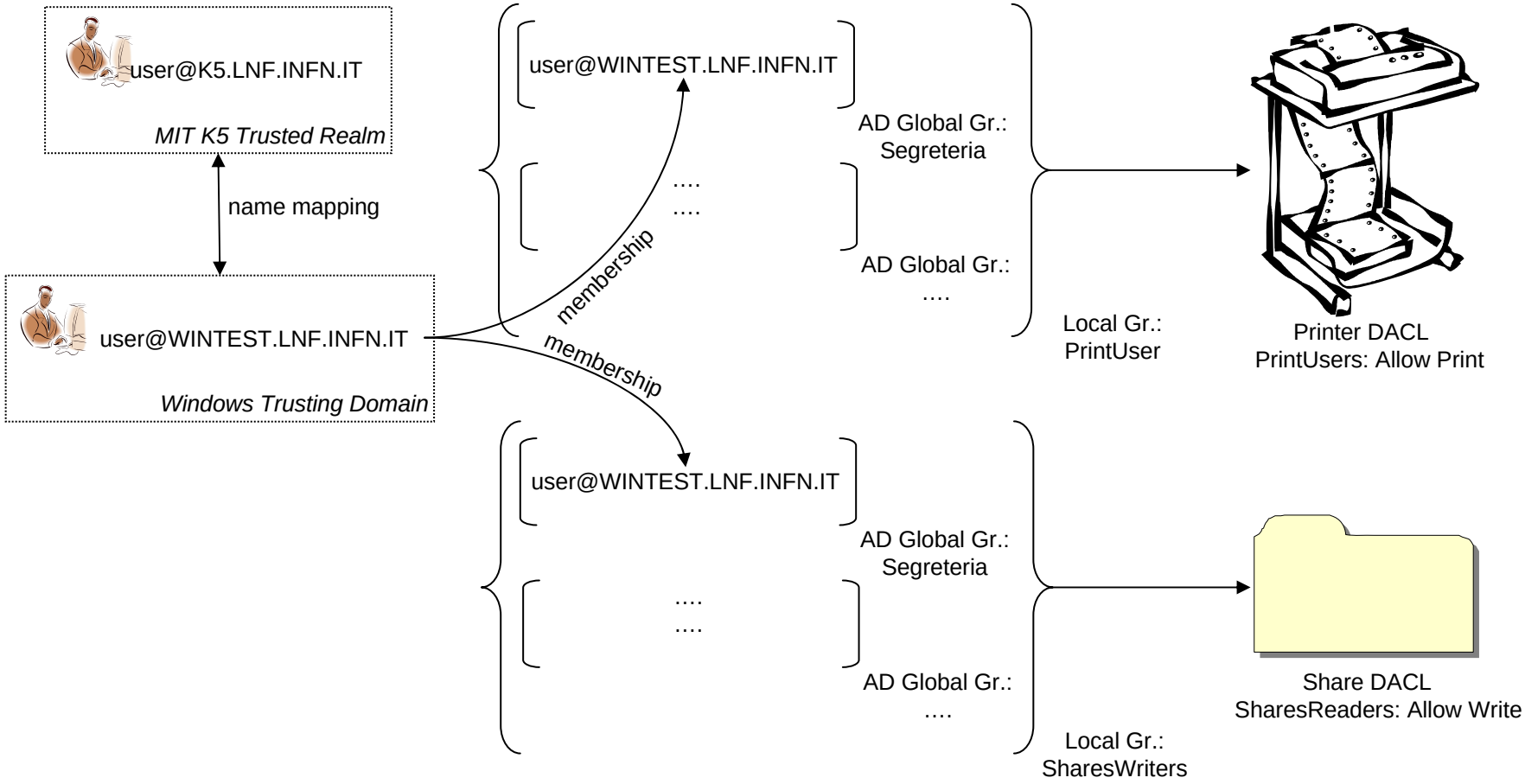
- All'utente che autentica nel regno trusted (MIT K5) deve essere associato un corrispondente account utente di AD
- Definire nel dominio (in AD e/o sui server membri) gruppi di protezione con ambito locale, ognuno relativo a specifico servizio windows
- Definire i diritti e i permessi di accesso, ai vari layers, relativi ai gruppi locali
- Pianificare i ruoli operativi, definendo per ciascuno un gruppo globale di AD
- Definire la memberships includendo gli account utente nei gruppi globali e i gruppi globali in quelli locali in base ai grantings desiderati

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - Global Case Study

W-Domain Groups Model

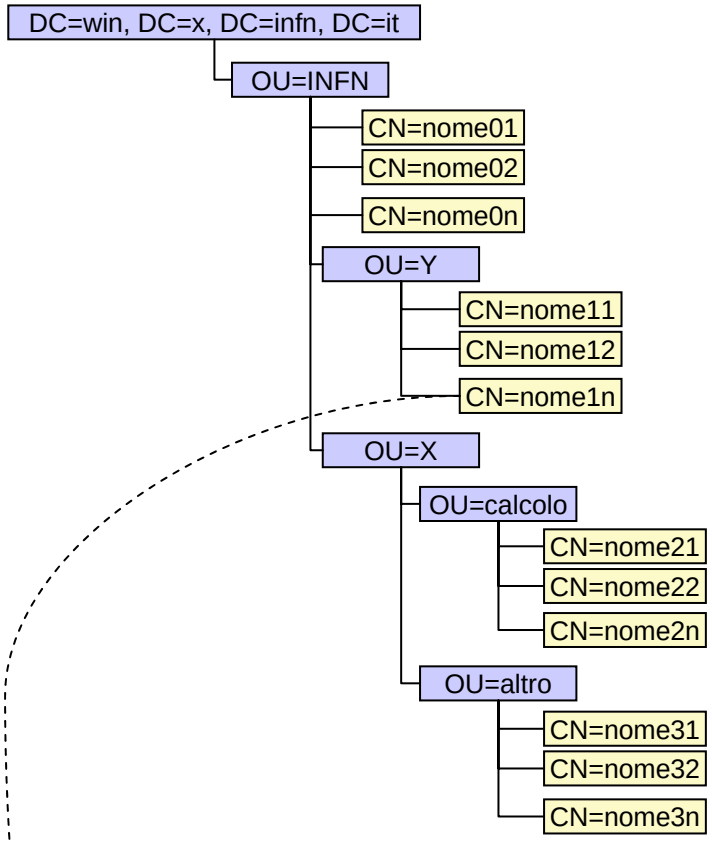
- I gruppi locali sono correlati ai servizi
- I gruppi globali sono correlati ai ruoli
- Ruoli distinti possono accedere allo stesso servizio
- Lo stesso ruolo puo' accedere a servizi distinti



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - Global Case Study

AD LDAP Names Space Layout

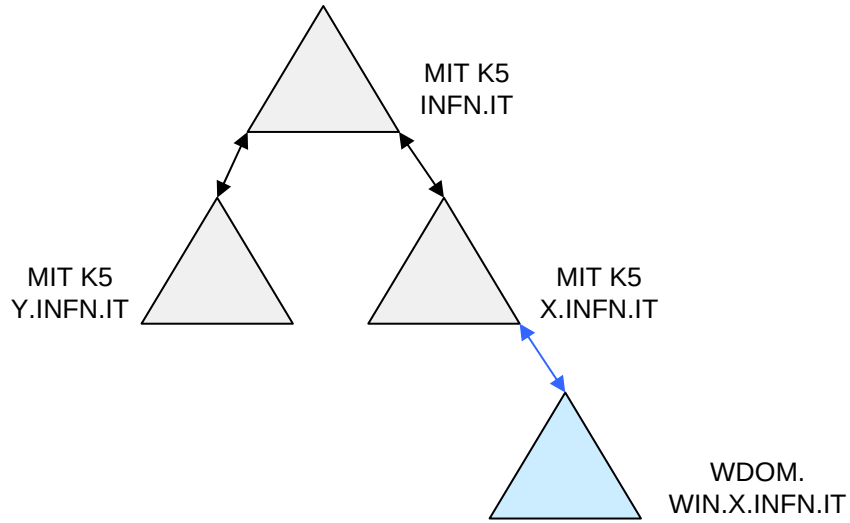


Nome Canonico windows: win.x.infn.it/INFN/Y/nome1n

LDAP: CN=nome1n, OU=Y, OU=INFN, DC=win, DC=x, DC=infn, DC=it

K5 user logon (principal):
- Windows: user1n@WIN.X.INFN.IT
- LX MIT: user1n@X.INFN.IT

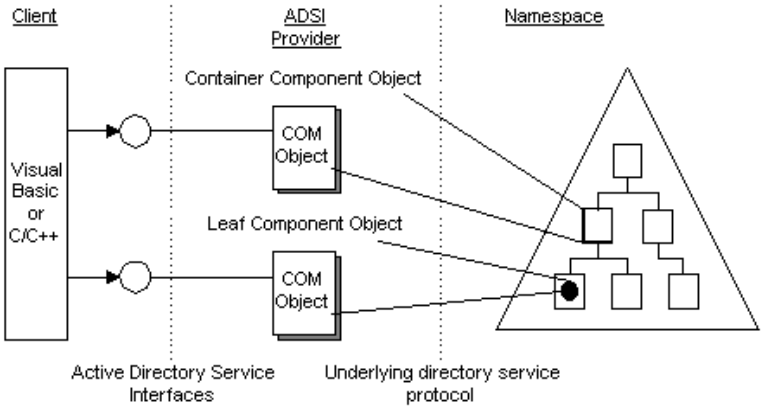
- Infrastruttura basata su unita' organizzative, associate ai regni di autenticazione MIT K5
- La OU relativa al Realm adiacente puo' essere strutturata in altre sub-OU associate ai gruppi Unix o AFS relativi alla cella locale
- Ogni OU contiene gli account windows mappati agli account nel corrispondente K5 Realm



Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - Global Case Study

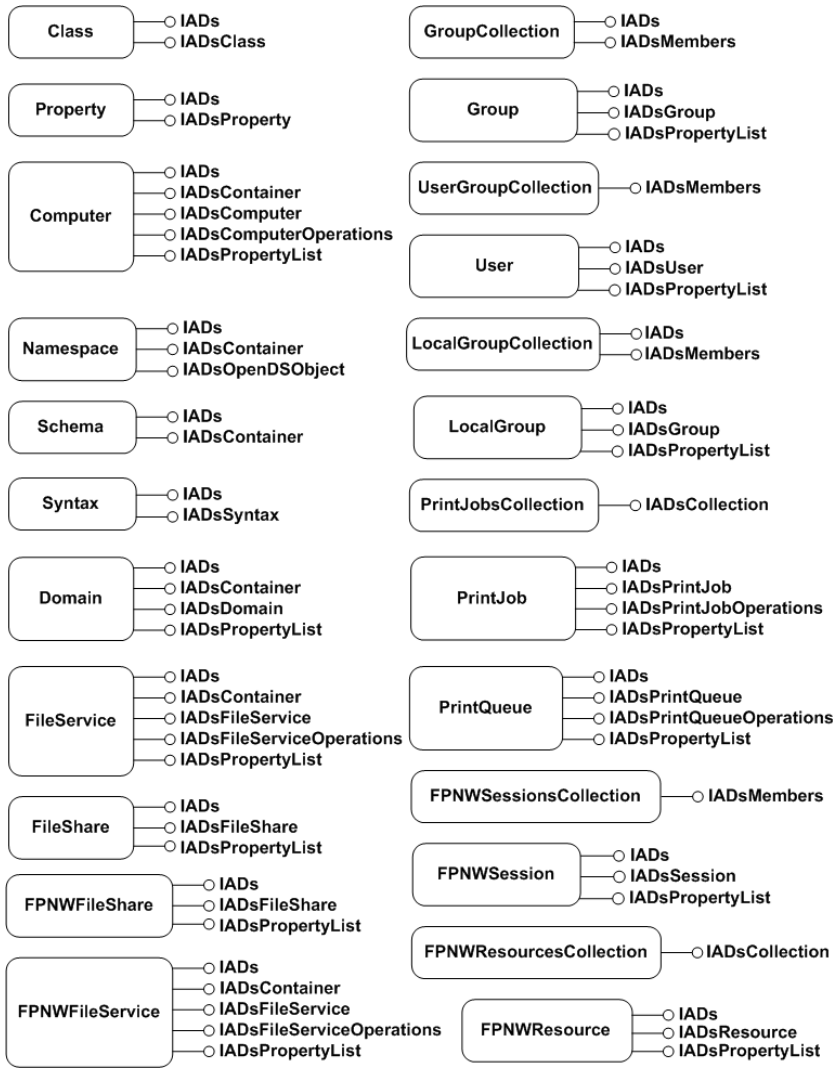
AD LDAP Names Space Implementation



ADSI Provider = interfaccia ad oggetti che esporta uno spazio di nomi di Active Directory

PROGETTO MANAGEMENT CONSOLE PER:

- Generare l'infrastruttura basata su OU
- Ricollocare gli account utenti pre-esistenti
- Creare nuovi account associati agli utenti trusted
- Attribuire agli utenti le memberships desiderate
- Intercettare/Monitorare gli eventi Kerberos e le relative queries



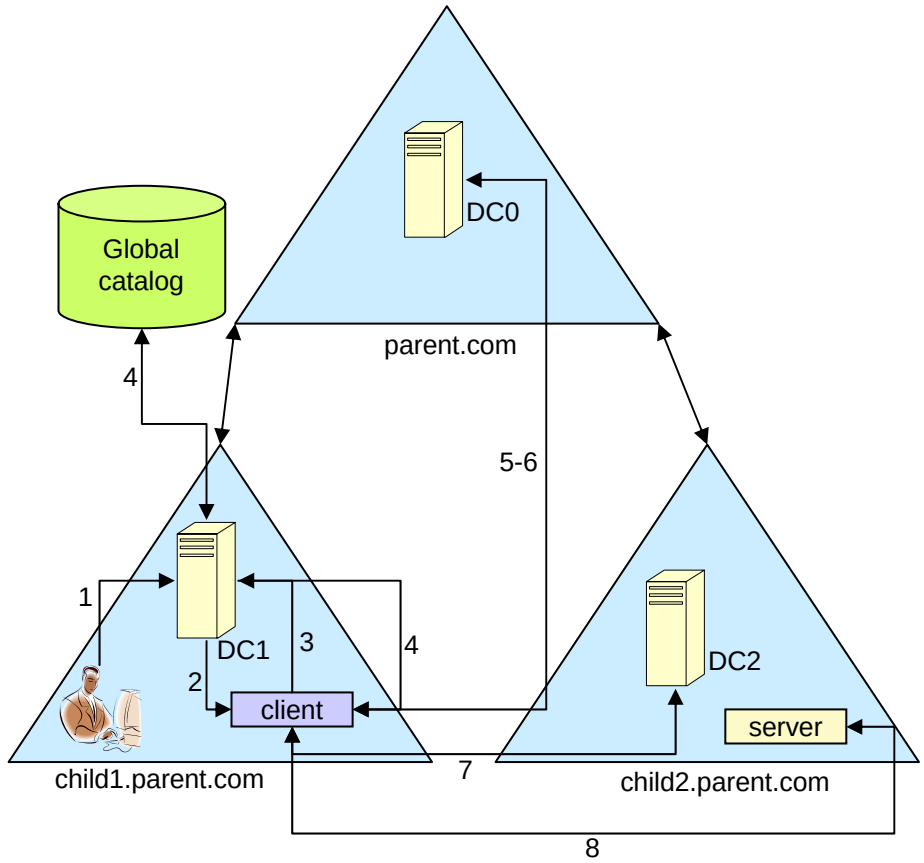
ADSI WINNT Provider Objects Model and Interfaces

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

3 - Global Case Study

W-Forest Trusts Tips

1. l'utente si autentica in child1.parent.com dalla postazione client.child1.parent.com
2. dc1.child1.parent.com rilascia un TGT
3. client.child1.parent.com richiede al TGS del suo dominio TGT valido per il TGS in child2.parent.com
4. dc1.child1.parent.com consulta il catalogo globale per determinare in percorso di autenticazione e rilascia un TGT valido per il TGS di dc0.parent.com
5. client.child1.parent.com presenta il TGT al TGS nel dominio parent.com e richiede un nuovo TGT per il TGS in child2.parent.com
6. dc0.parent.com puo' emettere il ticket richiesto in virtu' della relazione di trust
7. client.child1.parent.com presenta il ticket al TGS in child2.parent.com e ottiene un ticket per server.child2.parent.com
8. client.child1.parent.com presenta il ticket di servizio a server.child2.parent.com che rilascia un token di accesso

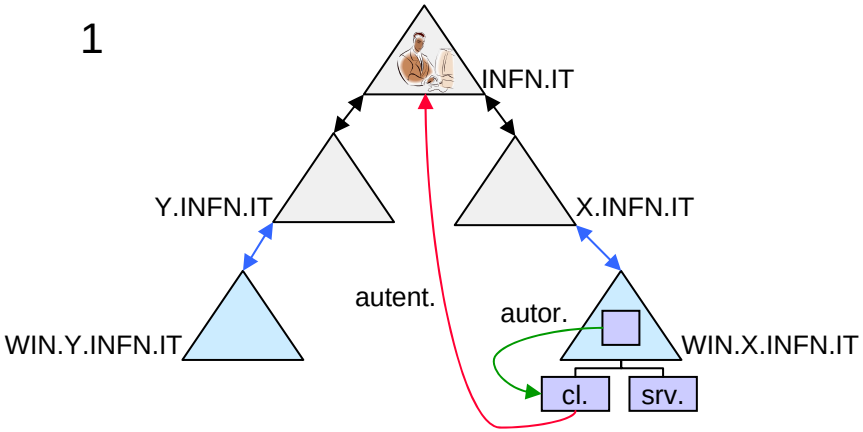


Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

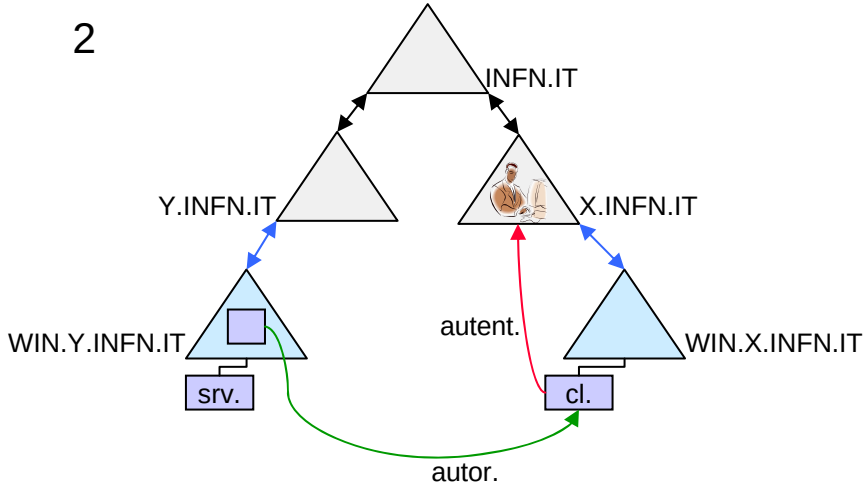
3 - Global Case Study

Mixed Realms Trusts Tests

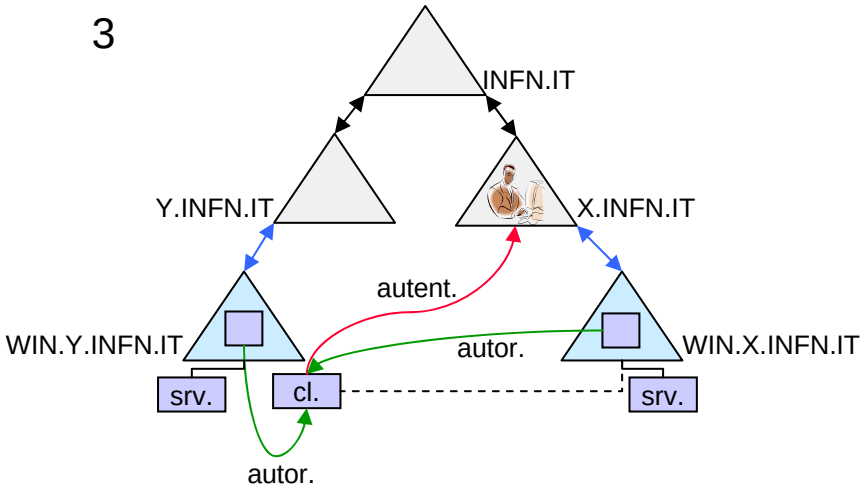
1



2



3



TEST GEOGRAFICI

1. Autenticazione in un Realm non adiacente e accesso nel proprio dominio dall'interno della propria Sede INFN
2. Autenticazione in un Realm adiacente e accesso in un dominio trusting esterno alla propria Sede INFN
3. Autenticazione nel proprio Realm, accesso nel dominio ospite e nel proprio dominio dall'esterno della propria Sede INFN.

Nunzio AMANZI - LNF Computing Service - Nunzio.Amanzi@lnf.infn.it

INFN
Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Frascati

Cordiali saluti

Nunzio AMANZI

Windows Systems Administrator
INFN SisInfo Management Team

LNF Computing Service