

# The INFN K5 project

HEPiX

BNL, October 18<sup>th</sup> 2004

Enrico M.V. Fasanelli



# Agenda

- A (little, I'll promise) bit of history
- The INFN K5 project and four W's on K5
- The status of the project
- Current activities
- Future plans
- The missing W
- Questions time

# The old history

- We have an heterogeneous authentication system
  - In the infn.it domain there are seven AFS cells: pi.infn.it, infn.it, le.infn.it, lngs.infn.it, Inf.infn.it, kloe.infn.it, roma1.infn.it
    - Only one K5 based
    - Two of them (lngs and Inf) are in a INFN LAB
    - Two of them (Inf and kloe) are in the same LAB
  - In the infn.it domain there are a 10th of Windows 2000/2003 domains (not too bad, it is always K5...)
  - A lot of any combination between NIS, WNT4, etc. etc.
- We “need” a better solution

# The “new” history

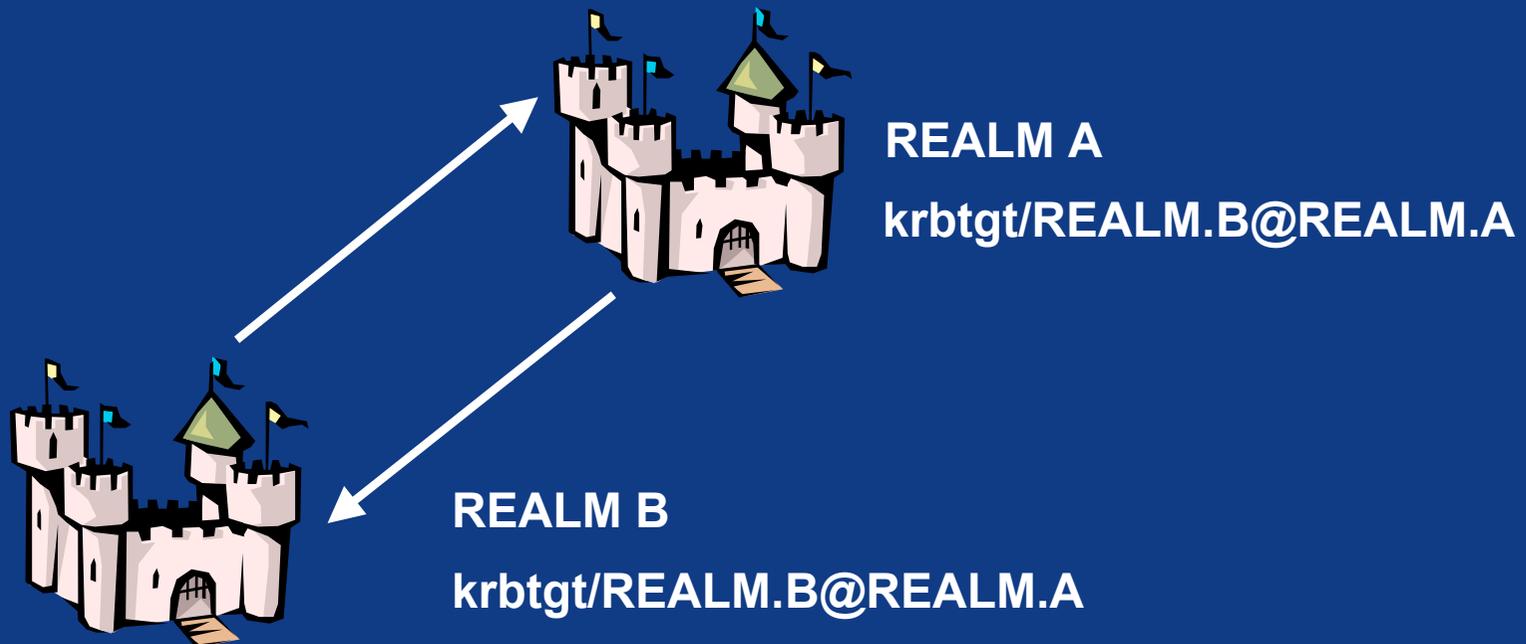
- INFN Lecce has the first K5 based authentication system (inside INFN) since 3Q01.
  - UNIX and Windows users use the same authentication system via trust relationship between LE.INFN.IT and W2K.LE.INFN.IT realms
- The new versions of OpenAFS (starting from 1.2.8) allow K5 authentication
- The new versions of MIT code (starting from 1.3.1) include support for OpenAFS
- The on WAN tests performed during 2Q03 show the feasibility of the “unification”
- New momentum in harmonization
  - Just before last autumn HEPiX, INFN CCR approved the K5 and TRIP projects

# The INFN K5 project

- Scope
  - Setup of a K5 based REALM INFN.IT and all necessary cross-realm trusts to be used - first of all - for the cross authentication of AFS cells
- Participants
  - 10 people, in 6 INFN sections
- Duration
  - One year
- Status
  - Approved in October 2003,

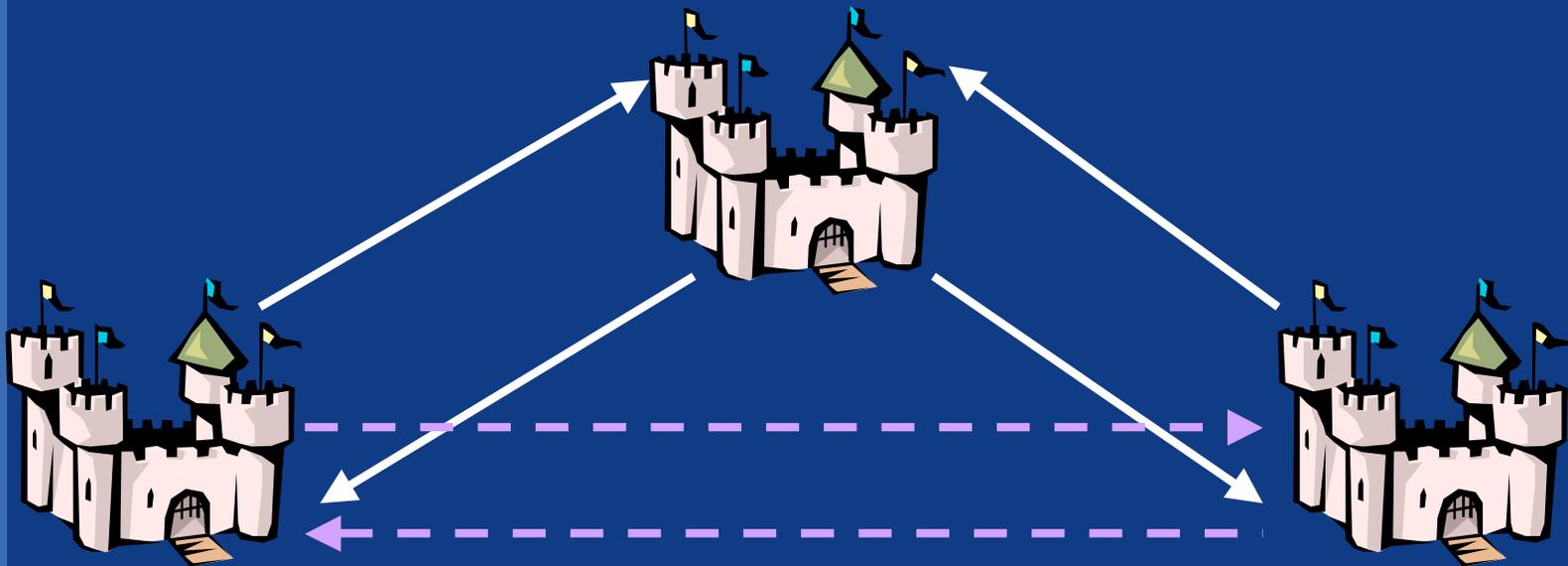
# Why K?

- Cross REALM trust relationship
  - Any principal in one REALM is authenticated against any other principal in the other realm
    - resource access (and then sharing) is “transparent”



# Why K5?

- Trust relationship IS transitive
  - Hierarchical in the same DNS domain
  - Via [CAPATH] Kerberos5 configuration between domains



# What K5?

- Requirements:
  - We need support for OpenAFS
    - Starting from version 1.3.1 MIT code includes AFS support
  - We need to be as compatible as possible with the Microsoft world
    - It is not a “secret” that Microsoft implementation of K5 is derived from MIT code
  - We need to be “safe” against changes due to “wrong” choice
    - Moving from MIT to heimdal is very simple, but the reverse seems to be not available
- MIT Kerberos5

# Where K5?

- We need to be as compatible as possible with our OpenAFS servers
  - RedHat Linux
    - Preliminary tests on 7.3 and 8.0
    - Last year setup on 9
  - Scientific Linux
    - Final setup
- We need to replace the 1.2.7-xx version with the 1.3.x one (AFS support and tools)

# When K5?

- Preliminary tests 2Q03
- Project submission 3Q03
- Project approved 4Q03
- Kick-off 1Q04
- Framework setup 2Q04
- Final tests 3Q04
- Production 4Q04

# Status of the project

- We setup the INFN.IT realm
  - Master KDC in CNAF
  - Slaves in PI, LE, LNF, ROMA1
- We tested user DB migration from KAS to K5
  - The tools coming with the MIT code works very well
- We defined DB propagation policy and we wrote a tool for that purpose
  - Use of `sgi_fam` (file alteration monitoring) for triggering the DB propagation
- We tested the cross authentication against a heimdal-based K5 realm (`caspur.it`)

# Current activities

- We are setting up the final REALM configuration
  - We are moving to SL
  - We are integrating the production infn.it AFS cell in the production INFN.IT K5 REALM
  - We are setting up all necessary trust relationships between INFN.IT and the existing K5 REALMs

# Future work

- Putting as many application as possible in this Kerberized framework
  - User login via kerberized ssh and telnet
  - File transfer
  - File sharing
  - Printing services
  - Roaming user authentication (TRIP)
  - Authenticated SMTP Relay
- Teach the users to use kerberized applications

# Who K5?

- In the INFN
  - The INFN AFS cell (nearly all INFN users)
  - INFN local AFS cell: PI, LE, LNF, LNGS, KLOE, ROMA1
- Inside HEP community, a lot of LABs and institution
  - FNAL, CERN, DESY, RHIC...

# Question time

- My questions:
  - Does it make sense to extend cross authentication outside the institution boundaries?
  - How can we coordinate?
- Your questions