Directory Services and Interoperability

A short chronicle of FAIL! :-)

Simo Sorce
Samba Team / Red Hat, Inc.

Directory Services

Centralize:

management of users

management of machines

control of security settings

configuration management

Windows – Active Directory

Good LDAP/Kerberos integration

Excellent support for Windows machines

Support for Linux/Unix machines

Good configuration management for Windows machines (Group Policies)

Linux / Unix

Good LDAP and Kerberos implementations but integration left to end-users *

Good support for Linux / Unix machines

No real support for Windows clients

No integrated configuration management but there are excellent solutions like Puppet

*FreeIPA is Red Hat attempt to fix this

Problems

Ownership of the Directory/Data

Semantics mismatches between OSs.

Custom Extensions/Data

Configuration management for different OSs.

What is FreeIPA ?

Why FreeIPA ?

IPA – Identity, Policy, Audit

FreeIPA is an integrated security information management solution combining 389 DS, MIT Kerberos, NTP, ISC Bind. It is managed through a web interface and command line tools.

What is FreeIPA ?

Currently supports users and credentials synchronization with AD domains through the DS winsync/passsync plugins.

Samba Integration is the next target.

Integration Strategies

Users replicated between AD and other LDAP

Samba4 on top of your LDAP Server

Trust relationship between AD and integrated LDAP/Kerberos/Samba solution

Replicating identities

Synchronization issues:

- out of sync trees
- conflicts
- single point of failure

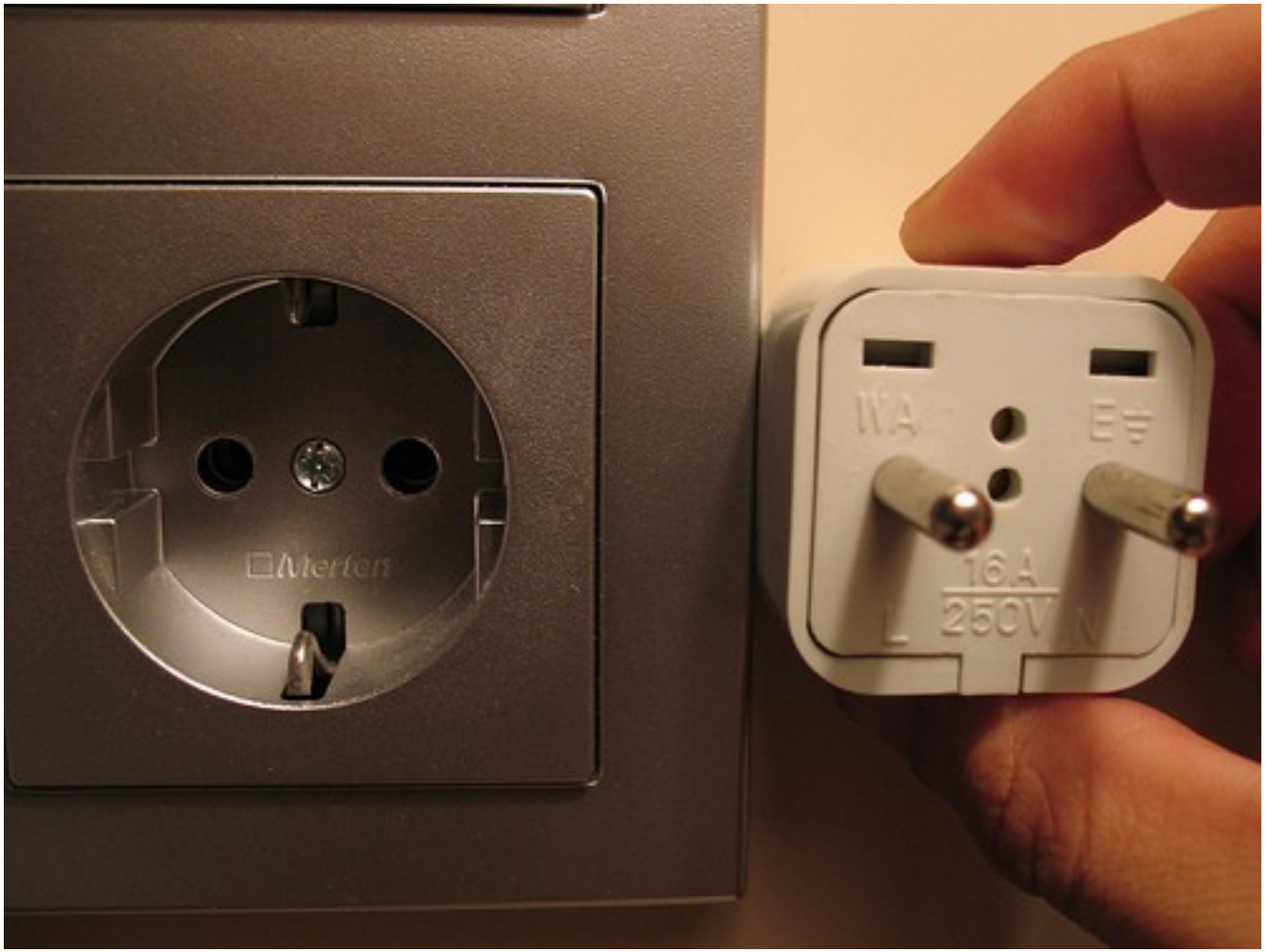
Groups?

- I want my own!
- Nested Groups ?
- Foreign Groups ?

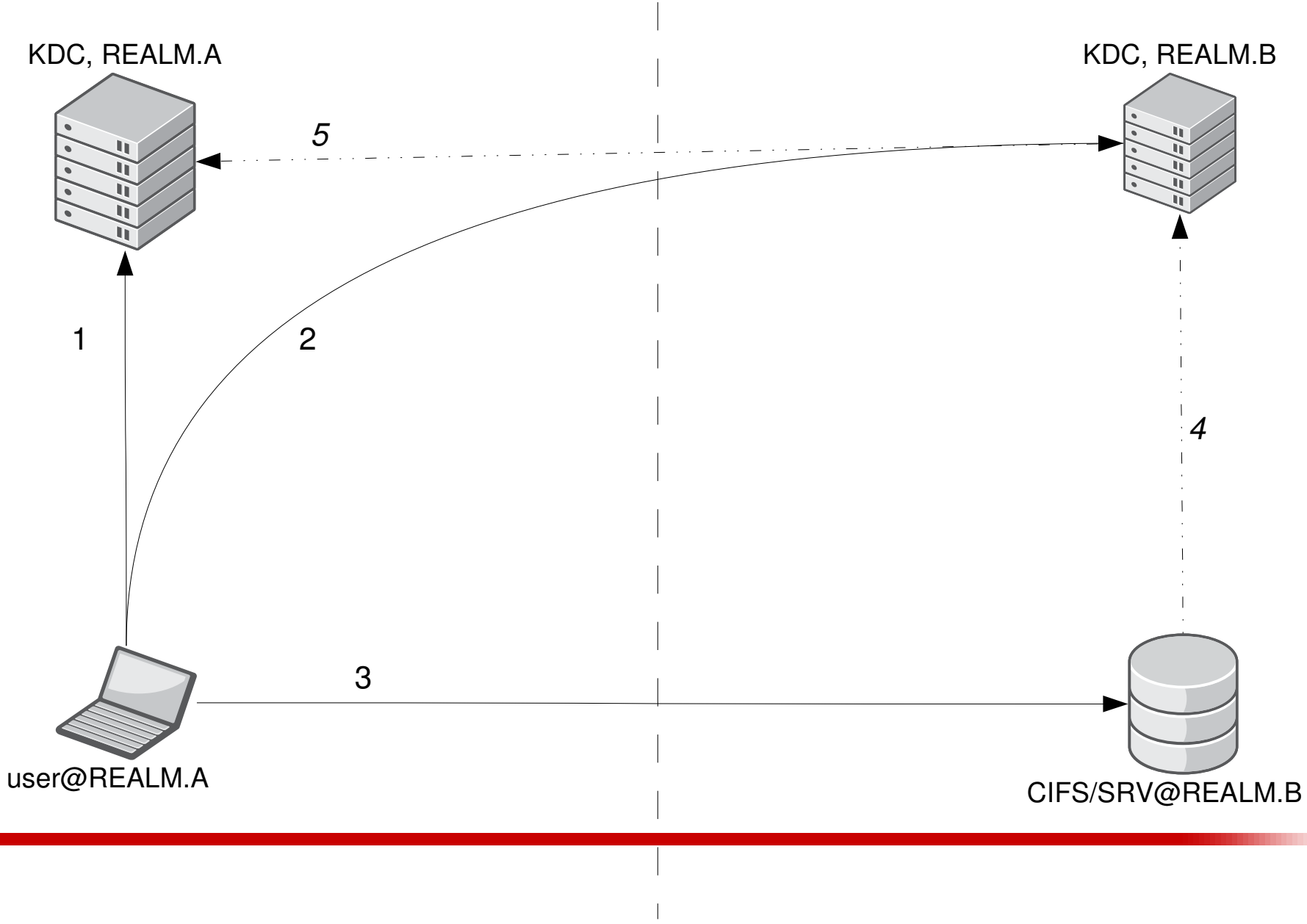
Authentication?

- password synchronization
- no Single-Sign-On

Samba-AD on pre-existing Directory



Trust relationship diagram



What kind of trust ?

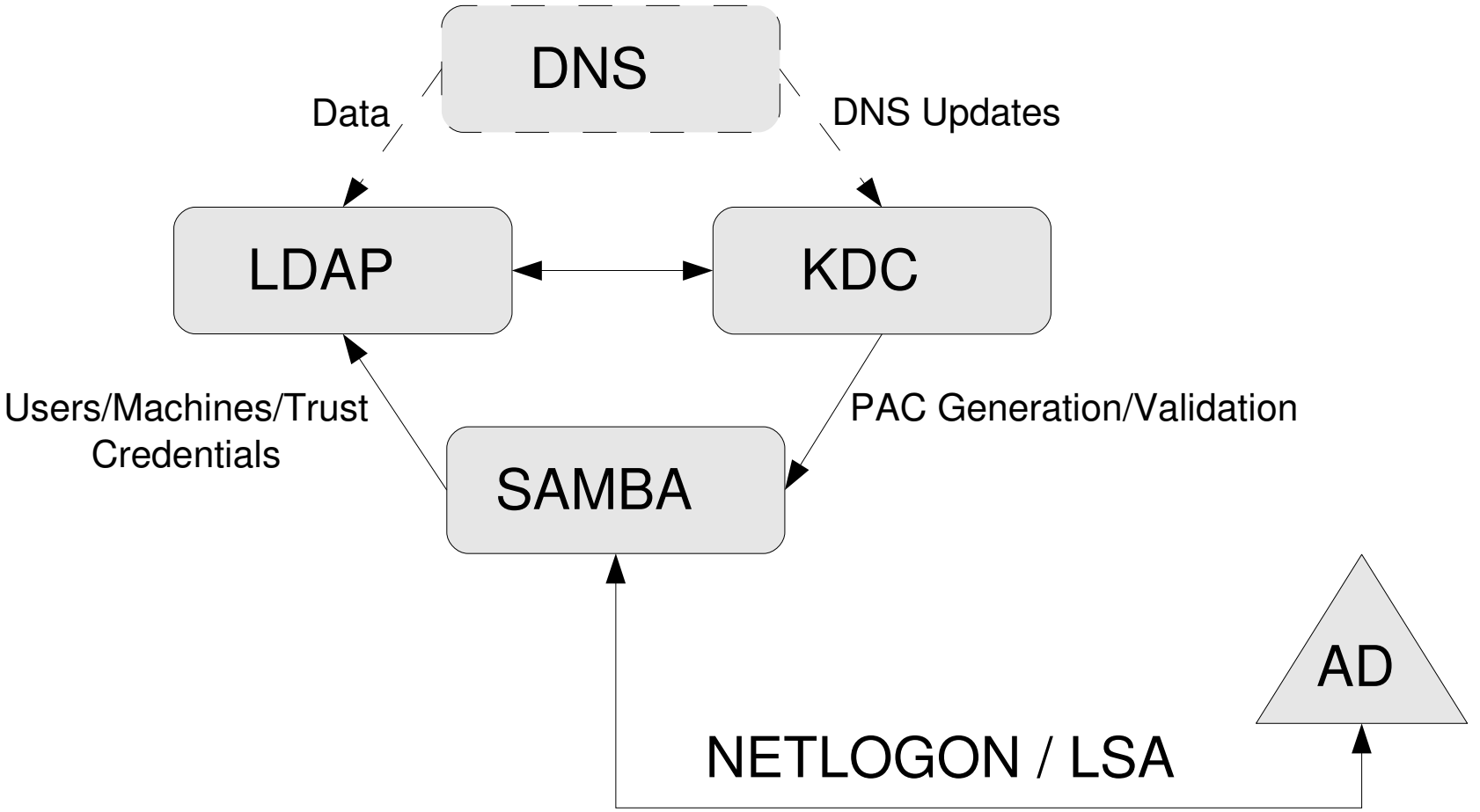
Simple AD-MIT Kerberos trust

Full External/Forest level trust

Required protocols for full AD trust

DNS
KRB5 (+MS-PAC)
NETLOGON
LSARPC
CLDAP(?)

What would it look like ?



Problems ?

Foreign domain users/groups

Custom groups to manage foreign users

PAC for Unix/Linux users that want to access Windows Resources

Questions ?

* Picture by user sfllaw from flickr, Creative Common Sharealike license