Cross-Realm Trust Interoperability, MIT Kerberos and AD

Dmitri Pal

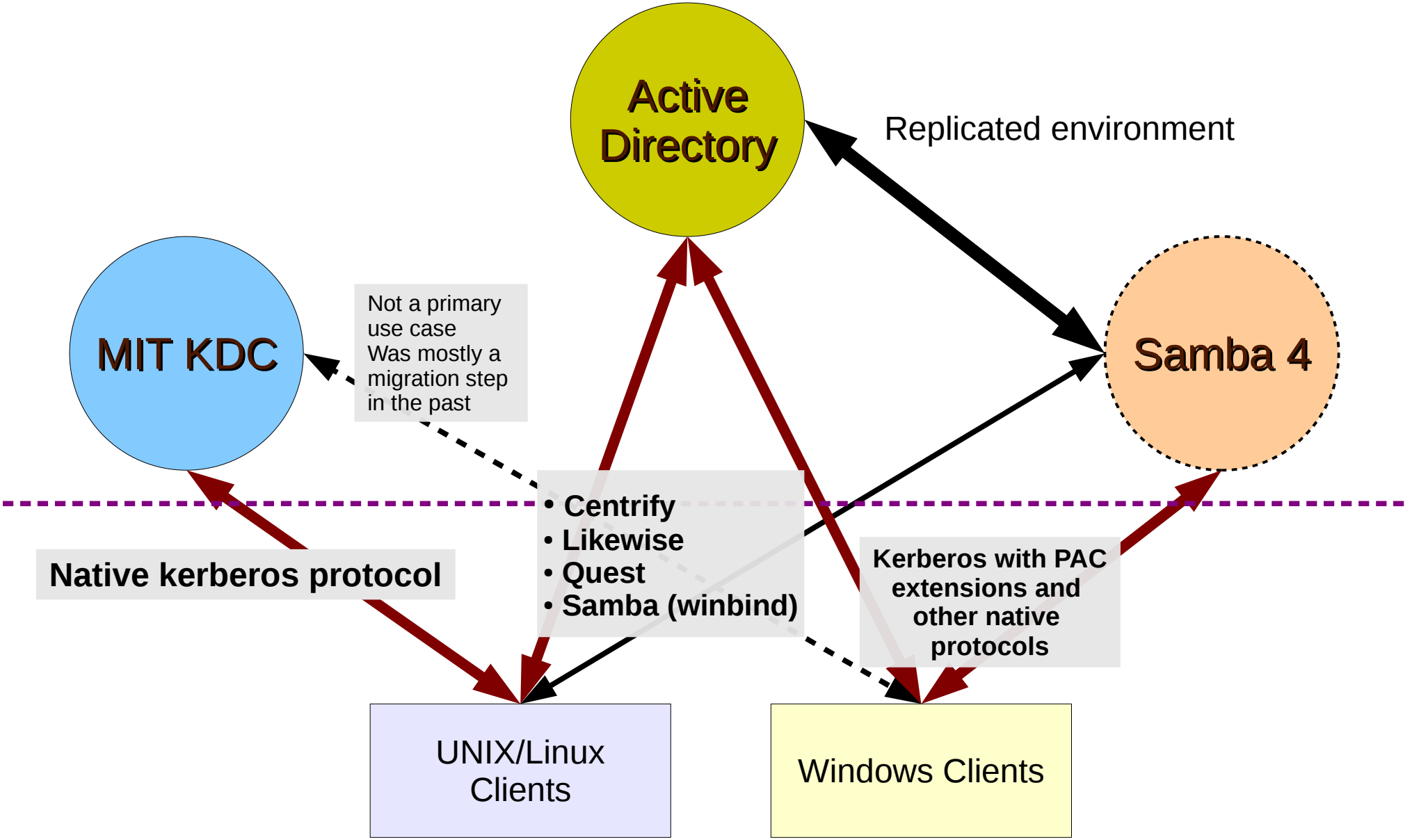
Sr. Engineering Manager

Red Hat Inc.

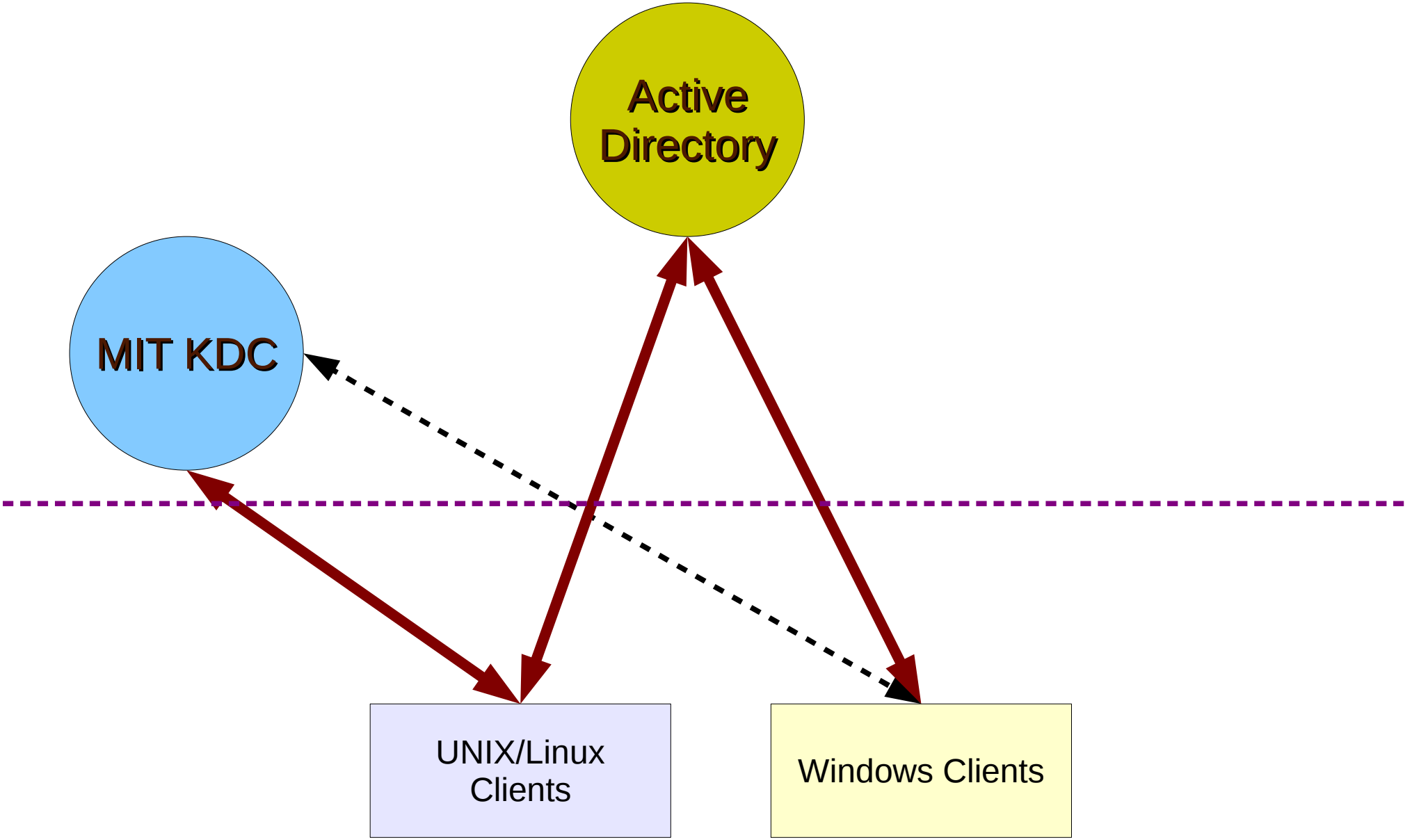
10/27/2010

What is our focus?

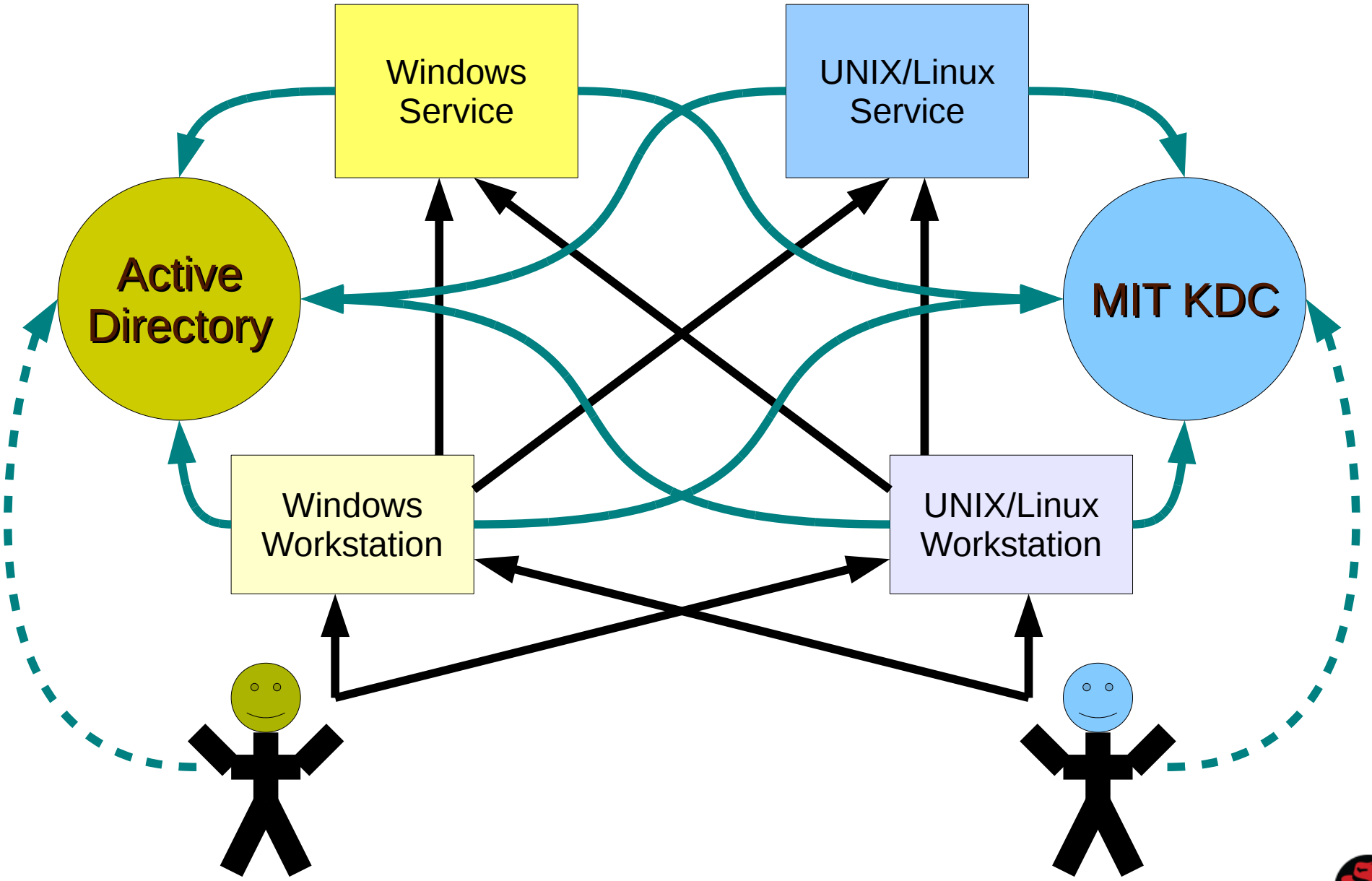
Traditional view on Kerberos interoperability



Simplified traditional view



Relations Between Two Domains



Use Cases

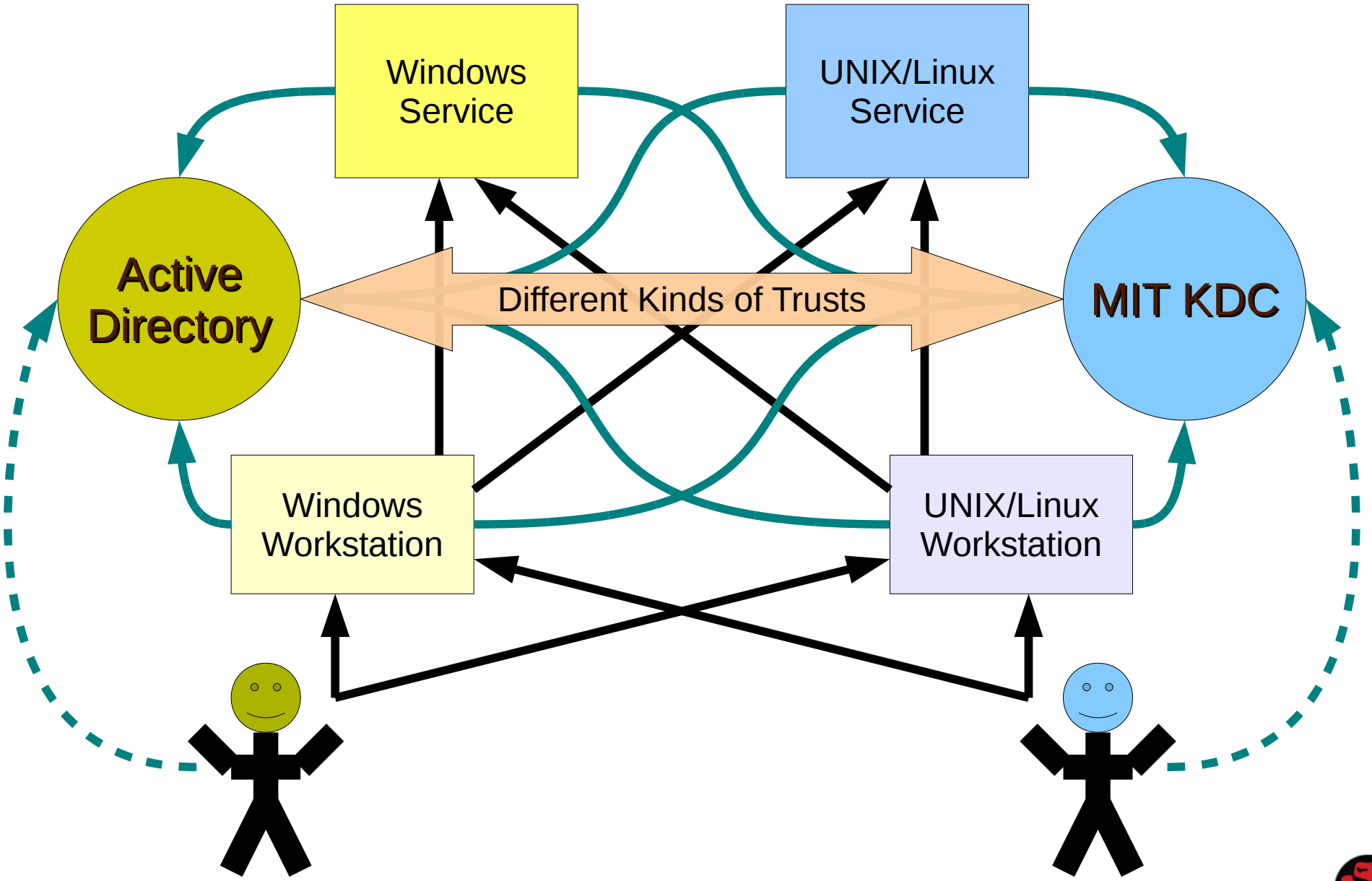
- Factors to take into the account

  Which domain X belongs? Where X is:

  - User
  - Desktop Windows vs Non Windows
  - Service Windows vs Non Windows

    Note: Different services/resources have different characteristics
- Actions:
  - Login... into which domain?
  - Access a service/resource... in which domain?

Relations Between Two Domains



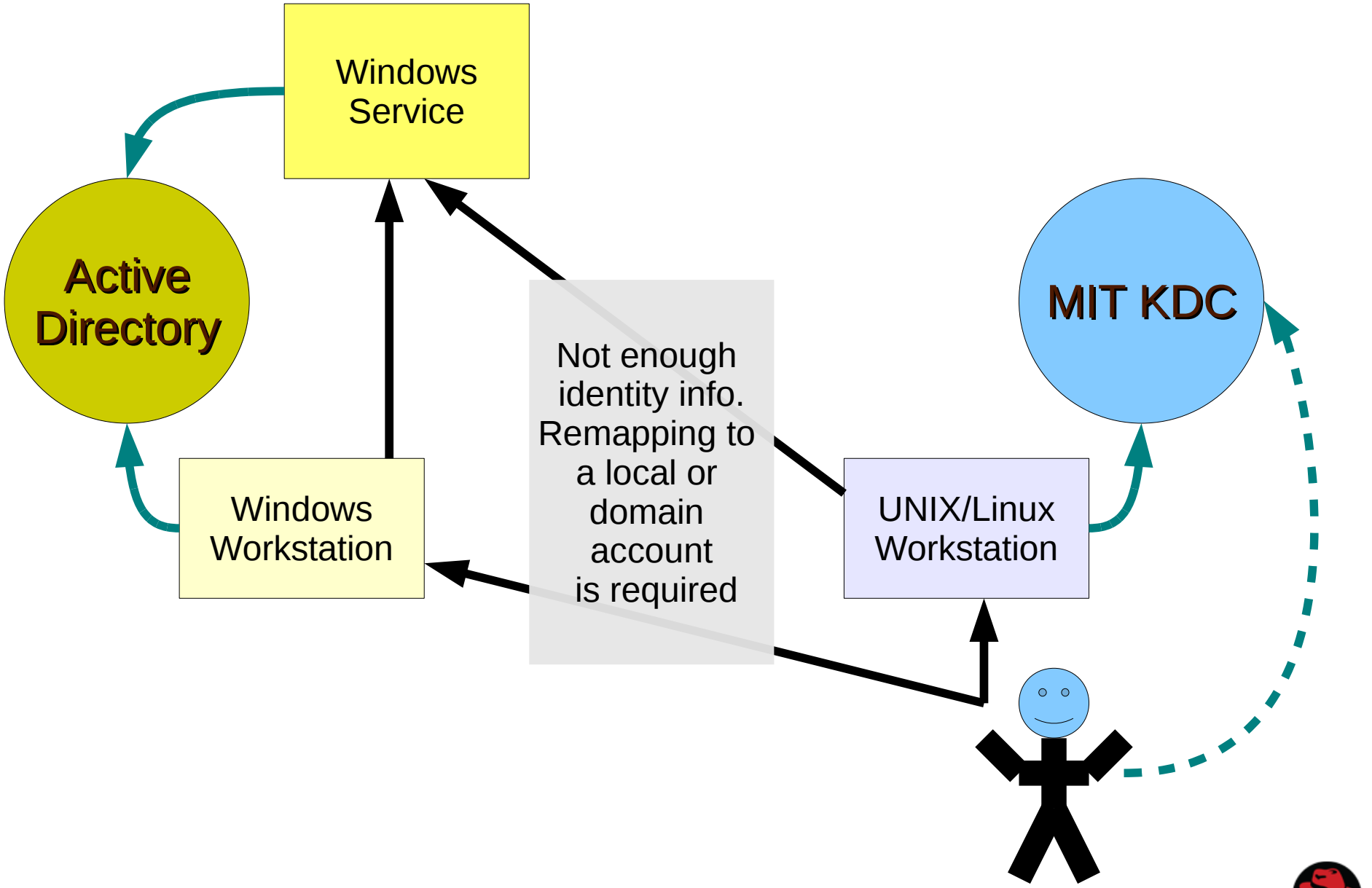
Closer Look at MIT Kerberos Approach

Current Situation

- Since the appearance of AD in Windows 2000, interoperability between MIT Kerberos Realms and AD domains has been a sort of one-way street.

- The reason is that there is no standard identity store that defines attributes needed by the OS in MIT Kerberos, therefore when using it in conjunction with Windows machines a mapping between local or domain accounts and MIT Kerberos principal names is necessary.

Lack of Identity Data



Closer Look at Microsoft Approach

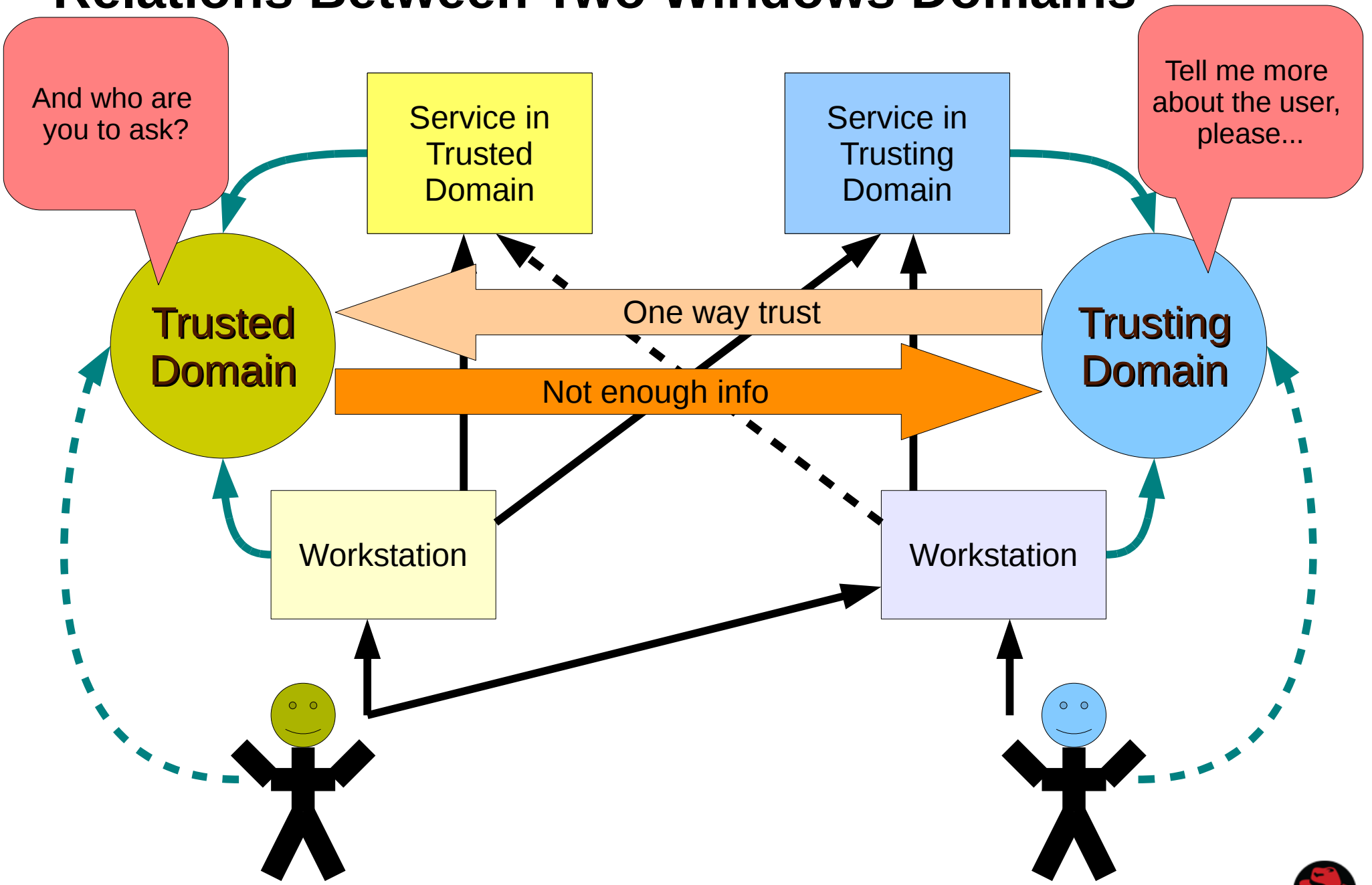
PAC – Privilege Access Certificate

- Problems:
  - Local users: remapping is not simple and not efficient
  - Domain users: lookups required for every operation
- AD Kerberos extension was born - called PAC
- Contains authorization information for the Domin User in the form of a list of groups the user is member of, and some other accessory information useful at login time.
- PAC solves both problems and helps with the trust use case.

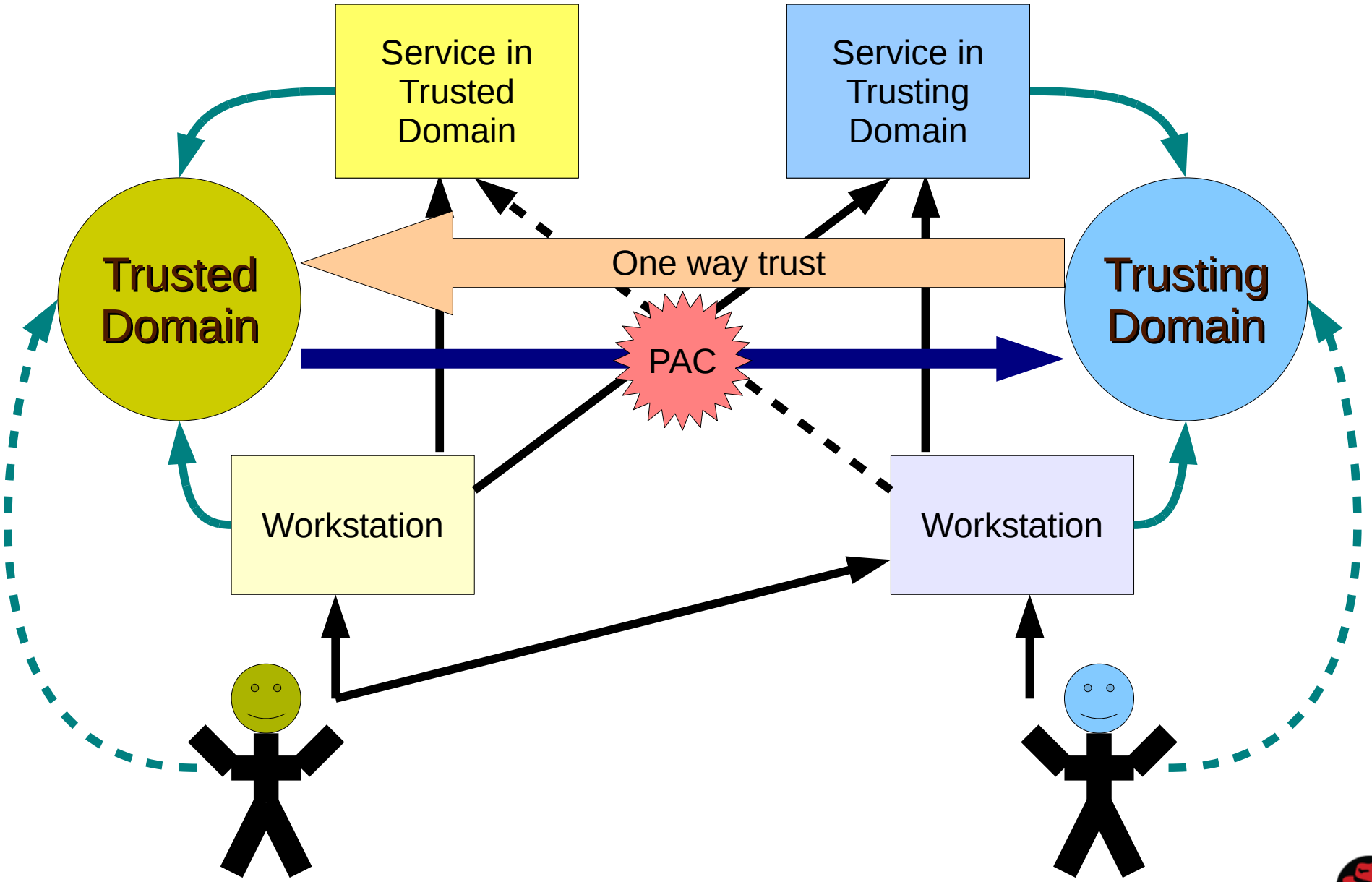
PAC and Trust Relationships

- Microsoft Windows Domains have always supported the concept of one-way trust relationship, even before Kerberos was introduced with Windows 2000 Servers.
- When a one-way trust relationship is established, computers in the trusting realm do not have any privilege over the trusted realm. At most anonymous connections can be established. This means that “querying back” for user information is either not possible (the trusted realm does not release this information anonymously or trusting client has no network access to trusted realm Domain Controller) or it is risky (anonymous connections).
- When authorization information travels with a Kerberos ticket, machines do not require access to the other realm anymore, the information is already available.

Relations Between Two Windows Domains



Microsoft Solution to Trusts



Back to MIT Kerberos...

Open Questions

- What are the options regarding domain trusts in MIT Kerberos without PAC?
  - Remap users?
  - May be synch?

Mapping Users and Trusts Relationships

- One way to do trust relationships between Windows machines and MIT Kerberos realms is by mapping Windows users to MIT Kerberos principals.
- This is really possible though only if both realms are homogeneous and represent the same user-base. It basically makes the MIT realm a shadow copy of the AD realm.
- But, if you have 2 different user bases one using Windows AD and the other based on a different directory and using MIT Kerberos for authentication, mapping is less then ideal.

Synching Directories

- Synchronizing is more difficult than it may look at first glance. The task that you never can get right... There is always something going wrong with it.
- The reason to have separate directories is generally to be able to better serve the user base, control authorization for the specific group of machines bound to the directory and in general be administratively independent.
- Synchronizing two directories makes most of these points moot. It makes the solution more complex (replication delays) and fragile, and less flexible.
- Groups are shared so authorizations decisions become common issues, not per realm properties as you would want/expect. Independence is lost.

More Use Cases to Worry...

Resource Domains Use case

- One concept often used in the Microsoft World is that of Resource Domains.
- A Resource Domain is a domain that is explicitly separate from the Domain where regular users are registered.
- Although historically Resource Domains were created more out of necessity (due to limitations in NT Domains technology), they also serve the purpose of allowing a very clear separation in Administrative responsibilities.
- Resource and Trusted domains are still used where organizations have clearly separate domain of administration. Users/desktops vs. Servers/Production machines vs. R&D labs.

Production Servers as a Separate Trusted Realm

- Generally the Windows desktop admins and the Linux server admins are separate divisions within the organization, but more importantly they have different requirements and skills and deal with different environments.
- The threats of a production server exposed to the outside world can be very different from those of the desktops within the corporate walls.
- So these two “domains” have very different characteristics, use different technologies and have different security requirements.
- Because servers may be more exposed, one-way can be seen as an appropriate measure to mitigate security breaches consequences.
- But without additional user information passed back about user the solution might not work. It depends on a kind of a service.

The Beginning...

FreeIPA as a Way to Manage UNIX/Linux Machines

- Red Hat has been sponsoring the FreeIPA project as a way to make it easy to manage group of Linux/Unix machines.
- FreeIPA relies on many existing components and marries an LDAP directory with the MIT Kerberos KDC.
- The aim is to build a system that can be easily used by Linux/UNIX admins and has built-in facilities to address natively the needs of Linux/UNIX administration.
- Therefore the focus is on managing Linux/UNIX servers and workstations.
- It goes beyond pure authentication and deeply involved in serving identity information used for access control.

FreeIPA and AD

- While FreeIPA is focused on managing Linux/UNIX servers it is also clear that in many enterprises, actual desktops are Windows machines managed through AD domains.
- It is clear that interoperability between FreeIPA and AD is therefore a necessity.
- The main challenge is to make it possible to allow an AD domain user logged on a Windows client, to transparently access a FreeIPA managed Linux/UNIX server without requiring the user to go thorough secondary authentication (SSO).
- At the same time we want to be able to make it easy for FreeIPA admins to manage Windows users access to Linux/UNIX Servers (authorization).

PAD – Principal Authorization Data

- What if we had a way to share authorization information?
  - We have recently started proposing a new standard to add a Kerberos extension so that authorization information can be transmitted in native format for POSIX machines. The PAD includes information similar to what is included in the MS-PAC.
- PAC<->PAD translation
  - In FreeIPA we are working to create a way to translate information coming from one side so that it can be reused natively on the other side. Without requiring kerberos clients to perform complex mappings on their own or contact foreign domains servers.
  - The idea is to allow the FreeIPA KDC to “translate” the MS-PAC that is sent from a Windows client when requesting a ticket in the FreeIPA realm, and substitute/accompany the original MS-PAC with a PAD that provides users/groups and login information in a format readily usable by Linux/UNIX client (POSIX attributes).
  - The inverse can also be done when a FreeIPA user wants to access resources in an AD domain.

Challenges

- Convince AD that we are a peer

  Setting up trusted realms in AD can be quite complex at the protocol level. AD trusts go beyond the classic exchange of passwords for the cross-realm trusts accounts, but involve also setting up routing information, dealing with referrals at the KDC level (instead of the client level), principals aliasing, and MS-PAC generation, validation and filtering among other things.

- Convince AD clients our users are legit

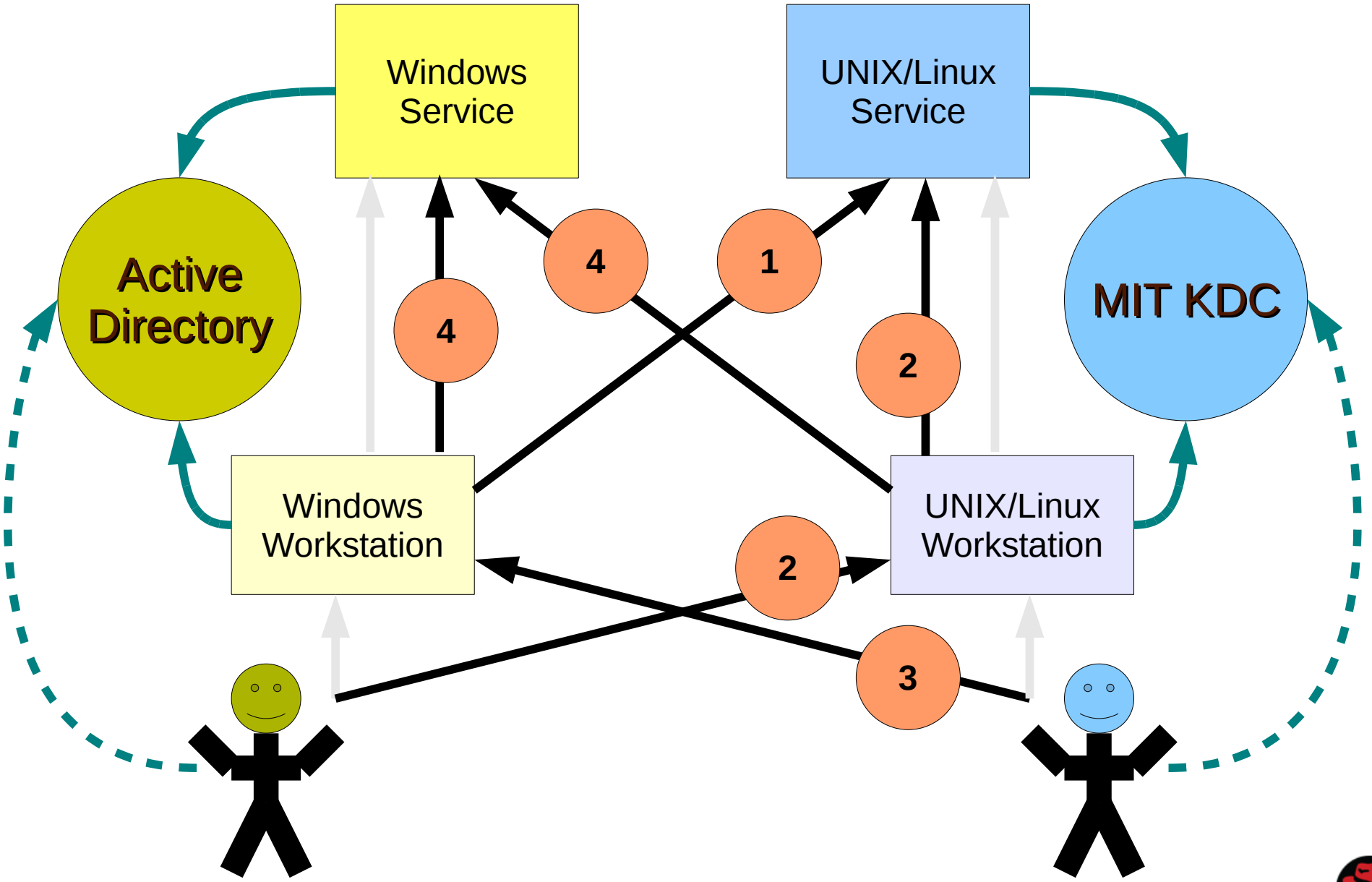
  In order to login into an AD managed client or server with a FreeIPA user we have to provide a MS-PAC to such client in the TGT. Failure to provide a client results in a cryptic error message at login time. In order to generate a valid MS-PAC we need to map POSIX UIDs/GIDs to Windows SIDs, by assigning a Domain SID to our Realm and add some other login related information into the mix. This operation can be done at the KDC level by providing a modified KDB plugin that is able to retrieve user data from the identity store (our LDAP server).

Goals in Priority Order

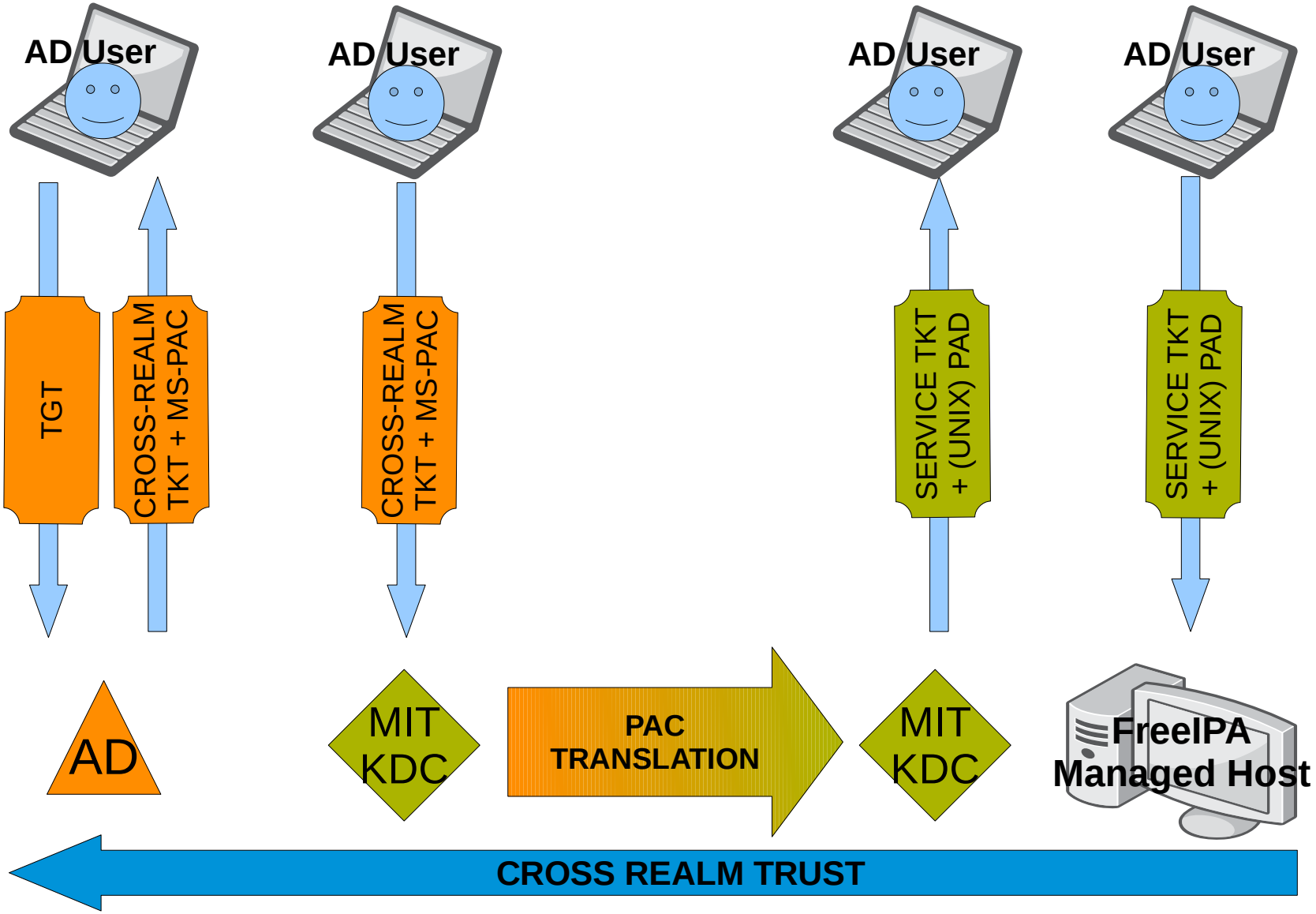
- AD users accessing services in the FreeIPA domain
- AD users logging into a UNIX box and accessing services in the FreeIPA or AD domains
- FreeIPA users logging into a Windows desktop
- FreeIPA users accessing Windows services

We will deal with them one at a time...

Illustration of Goals



AD user accessing FreeIPA managed host



Questions?