Plans for a single Kerberos service at CERN

Explanation and Timeline

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

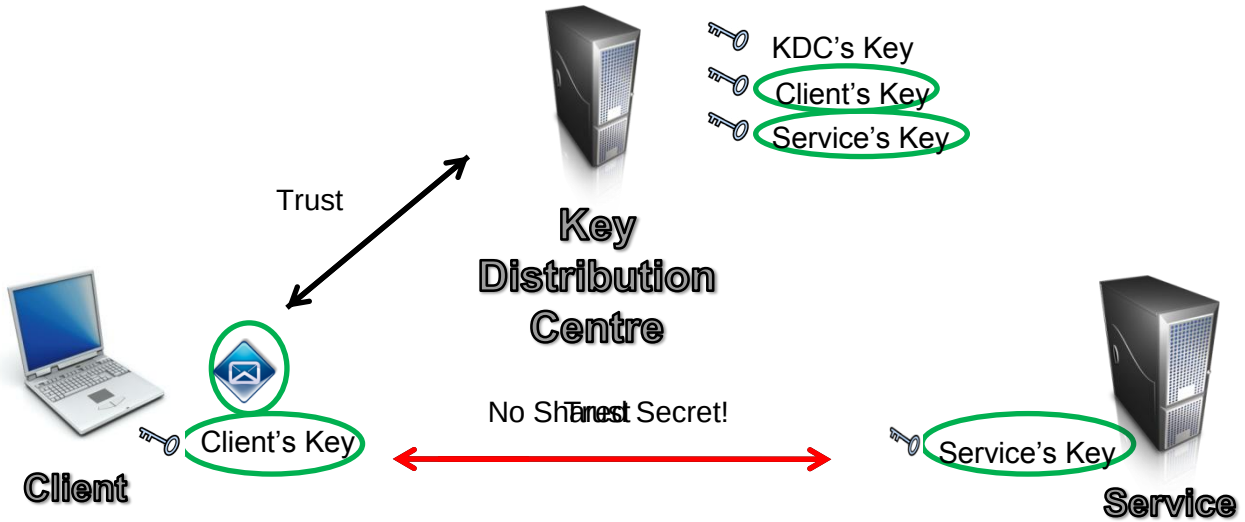
Agenda

- Short introduction to Kerberos
- The project
- Migration plan and impact

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Kerberos: Keys, Tickets and the KDC

- Kerberos uses shared secrets (keys) and tickets so that entities can prove their identities
- All entities (users and services) have a secret key, and a 'trusted third party' (the KDC) maintains a copy of all these keys
- Tickets are used to prove possession of keys and to distribute them, done by encrypting tickets and other data with the keys. Encrypting tickets ensures that only an entity with an identical key can decrypt and read the data



The Project

CERN IT Department

- Kerberized Services at CERN:

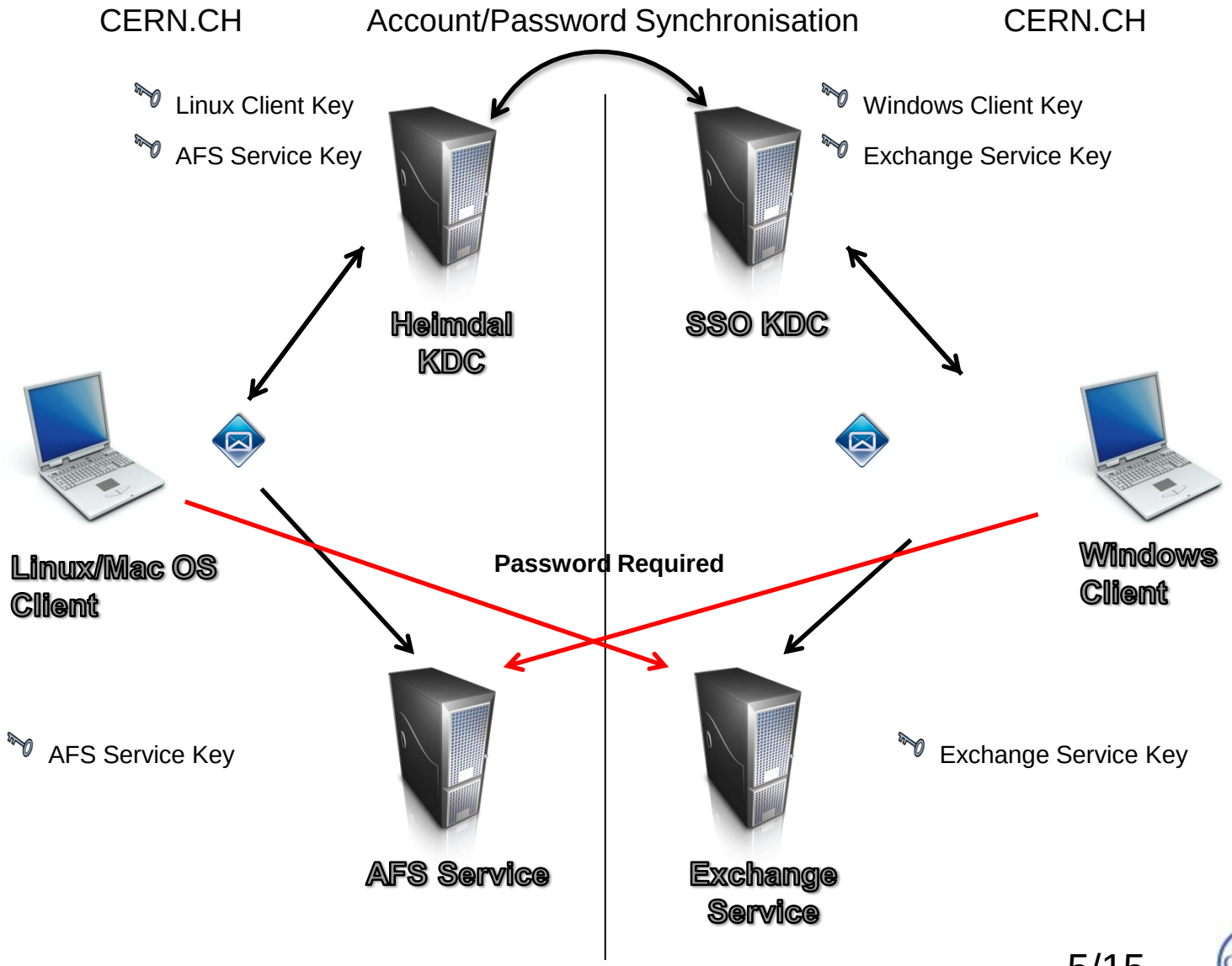
  Central Login, AFS, Exchange Server (e-mail), Web Single Sign On (SSO), LSF Batch, Acrontab, SSH (eg. lxplus,lxadm), CVS/SVN, CDB/SMS, DFS, …

- The problem
  - CERN IT runs two separate implementations of Kerberos
  - Some users and services are authenticating in one realm and the rest are in the other.
  - Therefore, not all services are available to all users with strong authentication and SSO
- The goal of this project is unify these two systems so that..
  - All users can access all services using strong authentication and SSO
    - E-mail
    - AFS
    - SSH
    - Web SSO
    - Future services…
  - No synchronisation between realms
  - Authentication services are managed by one IT group

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

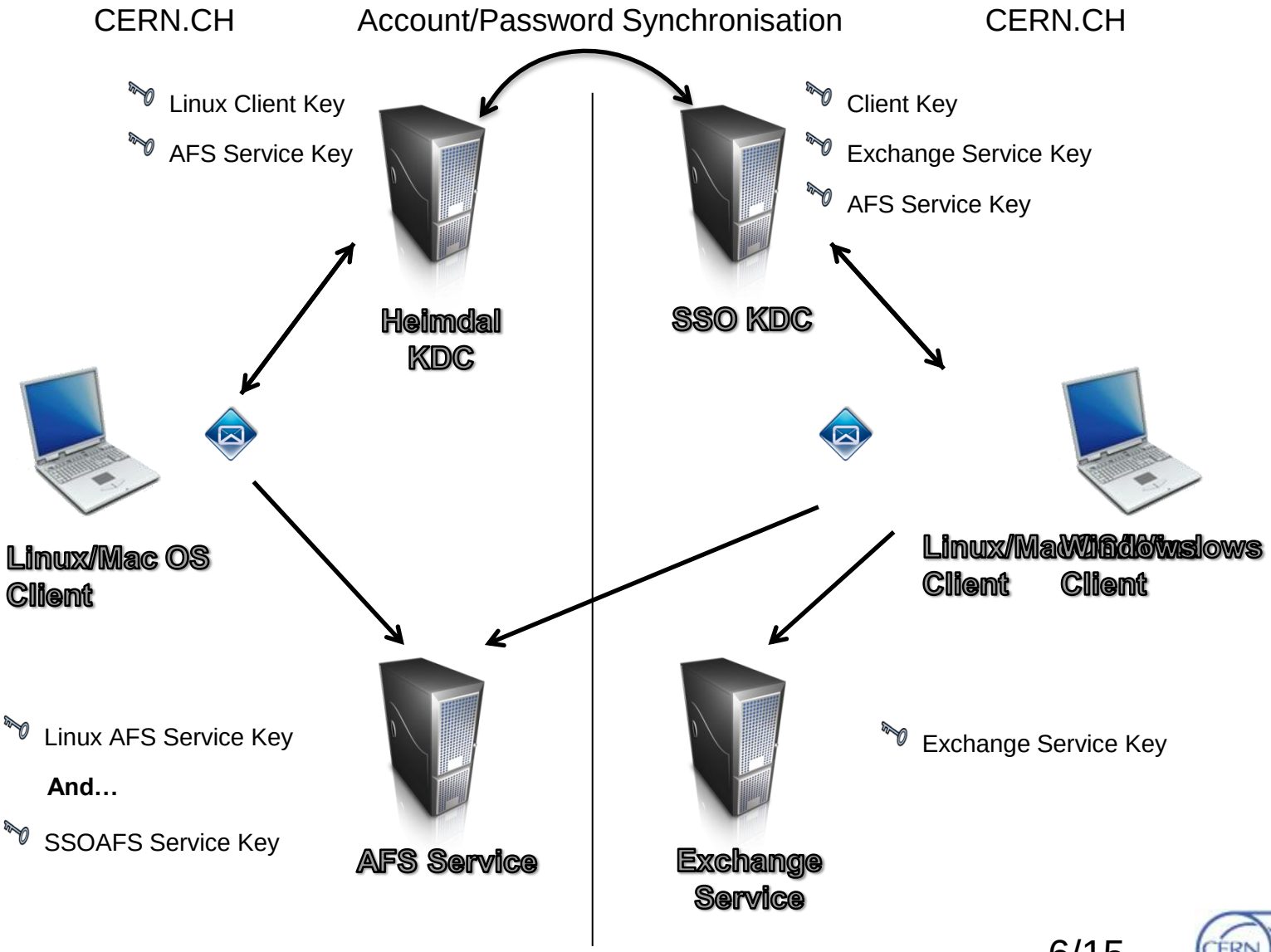
CERN

Kerberos authentication at CERN

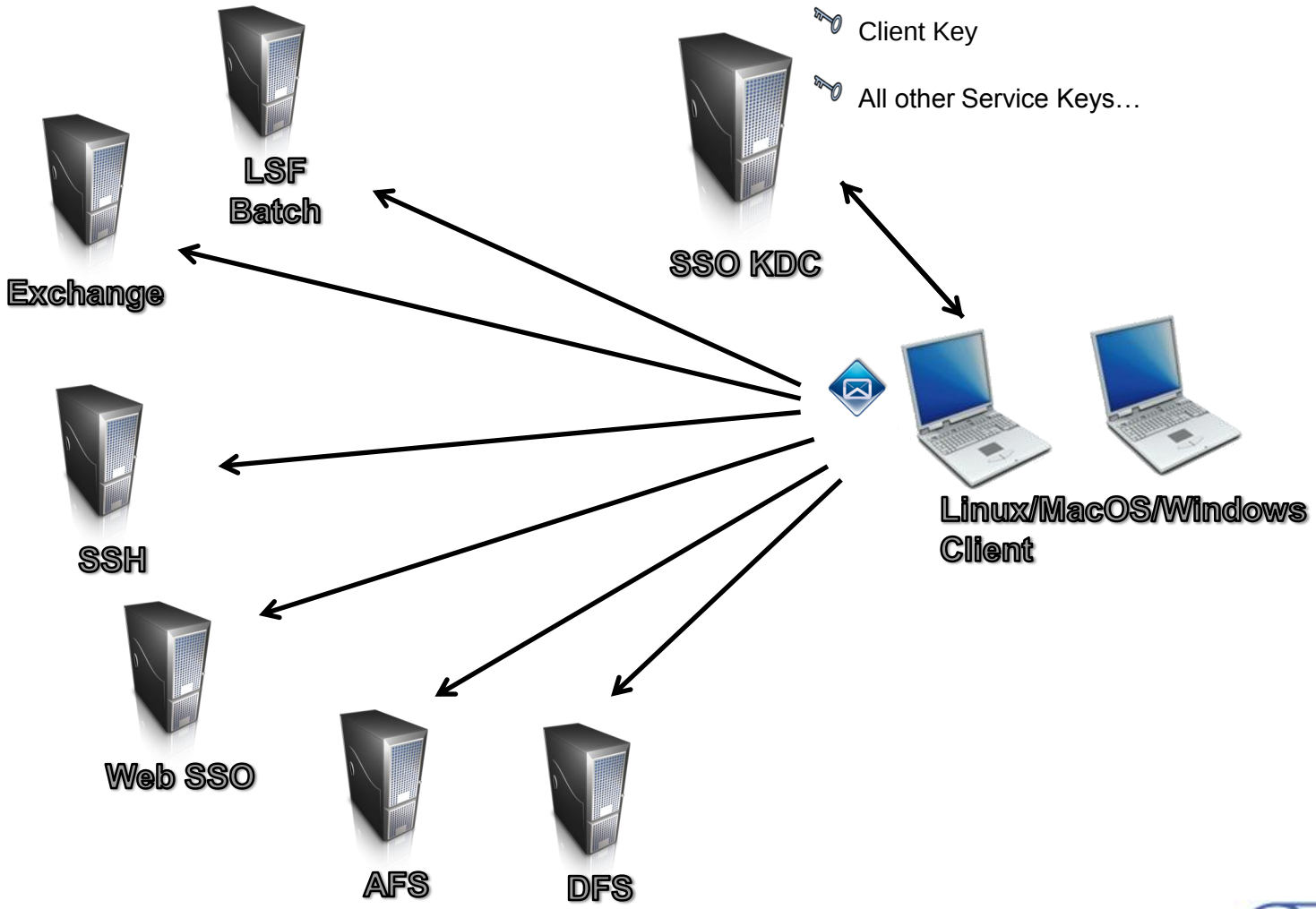


CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

To enable a site-wide migration



Post Migration



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Infrastructure Changes (1)

CERN IT Department

- Keytab Extraction
  - Keys are extracted for both realms using an ARC (Authenticated Remote Control) based system.
  - Clients interface with intermediary SLC5 server, which uses the msktutil software to contsruct a keytab and reset the corresponding computer account in AD.
- Acrontab (remote crontab system based on kerberos)
  - Client determines the origins of it's credentials and authenticates against the original acronserver to register the job (Heimdal), or to a frontend, which processes the request and registers the job on the client's behalf.
  - This allows for a unified 'crontab' to be maintained whilst clients authenticate with credentials originating from either realm
  - Acronserver will be switched post-migration to Active Directory only.

Infrastructure Changes (2)

CERN IT Department

- Batch Authentication - Batch nodes require access to fresh user credentials on demand, as their jobs may run for many weeks and they may be triggered a long time after the initial submission
  - Originally satisfied by straight keytab extraction/credential acquisition, but key extraction is not possible in Active Directory, without using a ‘hack’ such as thread injection into the LSA process to acquire password hashes.
  - Using the S4U Constrained Delegation protocol extension was considered, but inflexible and un-tested with the MIT implementation
  - Alternative acquisition system written based on PKINIT, with single x509 certificate mapped to all accounts in order to provide the same level of flexibility as is currently available. Certificate controlled by batch server, which securely distributes TGT’s to batch nodes on request and node has demonstrated it’s identity.
- Batch system authentication changed to allow for clients of either Kerberos flavour to register jobs and to have them ran on nodes of either Kerberos flavour

Infrastructure Changes (3)

- Dealing with credential/config mismatches during remote session credential delegation
  - Module written for the pam stack to detect and resolve mismatches between delegated user credentials and the server's Kerberos configuration.
  - Module detects TGT encryption type of delegated credentials and exports a Kerberos environment that allows further tickets to be acquired.
- For user keytabs (useful for local, longterm, Kerberos dependant tasks), a simple alternative to extraction has been written to construct keys for a principal using a (correct!) password provided.
- Dual-Boot systems (same account object in LDAP, with one key)
  - Investigating a system of disabling Windows client key updates and writing a tool to ensure both OS's use the same key client side.

Steps the Users must take

CERN IT Department

- Users on managed machines (Lxplus, lxbatch, slc4, slc5)
  - Nothing to do: Users are transparently moved to the new KDC
- Non Managed Machines
  - Users will need to edit their /etc/krb5.conf to point to the SSO KDC (Active Directory)
- Users requiring Self Authenticating Scripts (i.e K5Reauth):
  - Users must re-acquire a Kerberos key from AD using provided software

https://twiki.cern.ch/twiki/bin/view/AFSService/MigratingToActiveDirectory

Optional steps that might benefit users

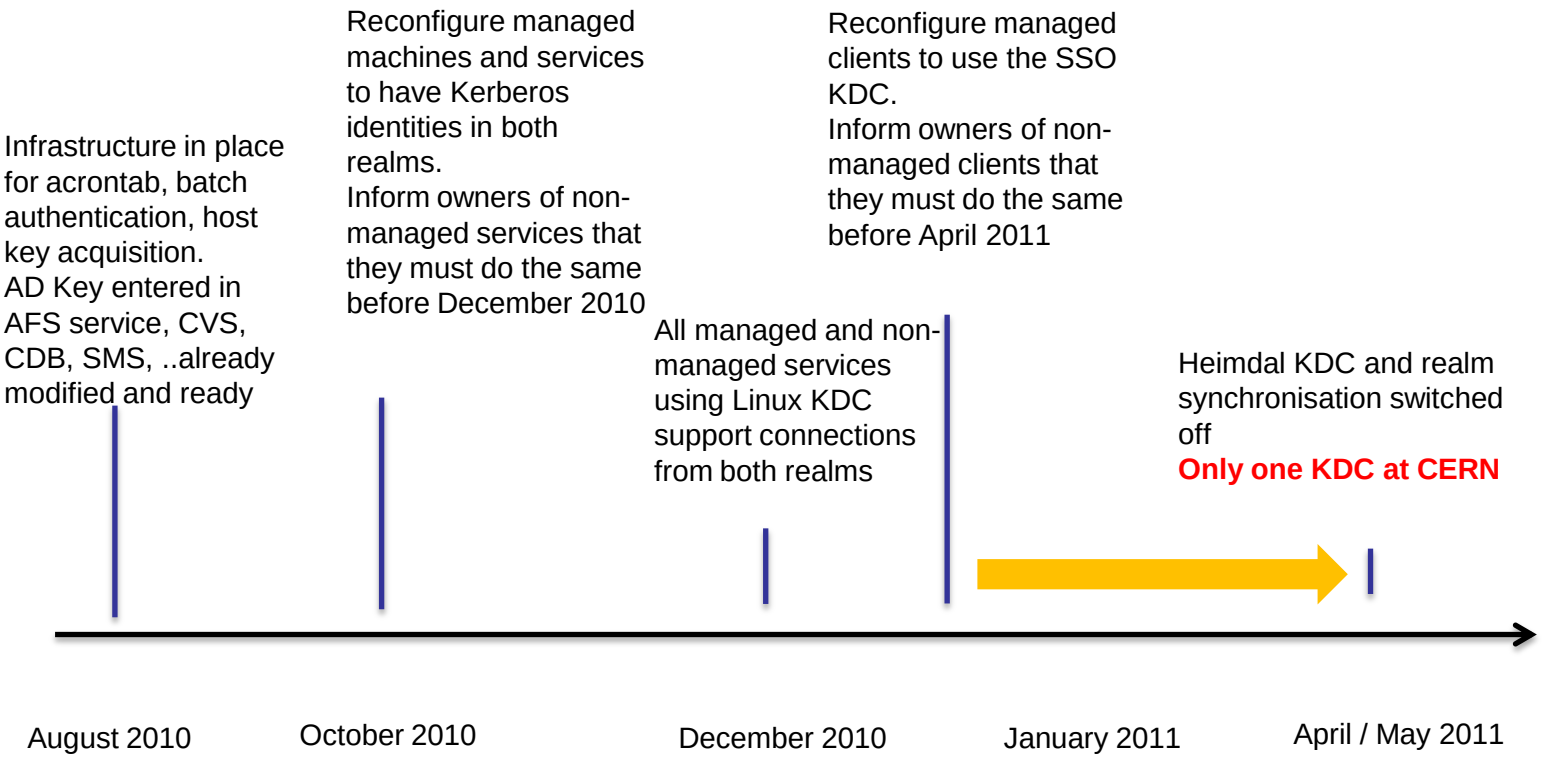
CERN IT Department

- E- mail configurations can be changed to use Kerberos for authentication, (al)pine, thunderbird and evolution have been tested.
- To use Kerberos for putty SSH sessions, get ‘Putty Quest’ from CMF or follow these instructions:

  https://twiki.cern.ch/twiki/bin/viewauth/AFSService/PuttyWithKerberos
- To use AFS for Windows, follow these instructions:

  https://twiki.cern.ch/twiki/bin/view/AFSService/InstallingOpenAFSClient

Roadmap



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Dealing with problems

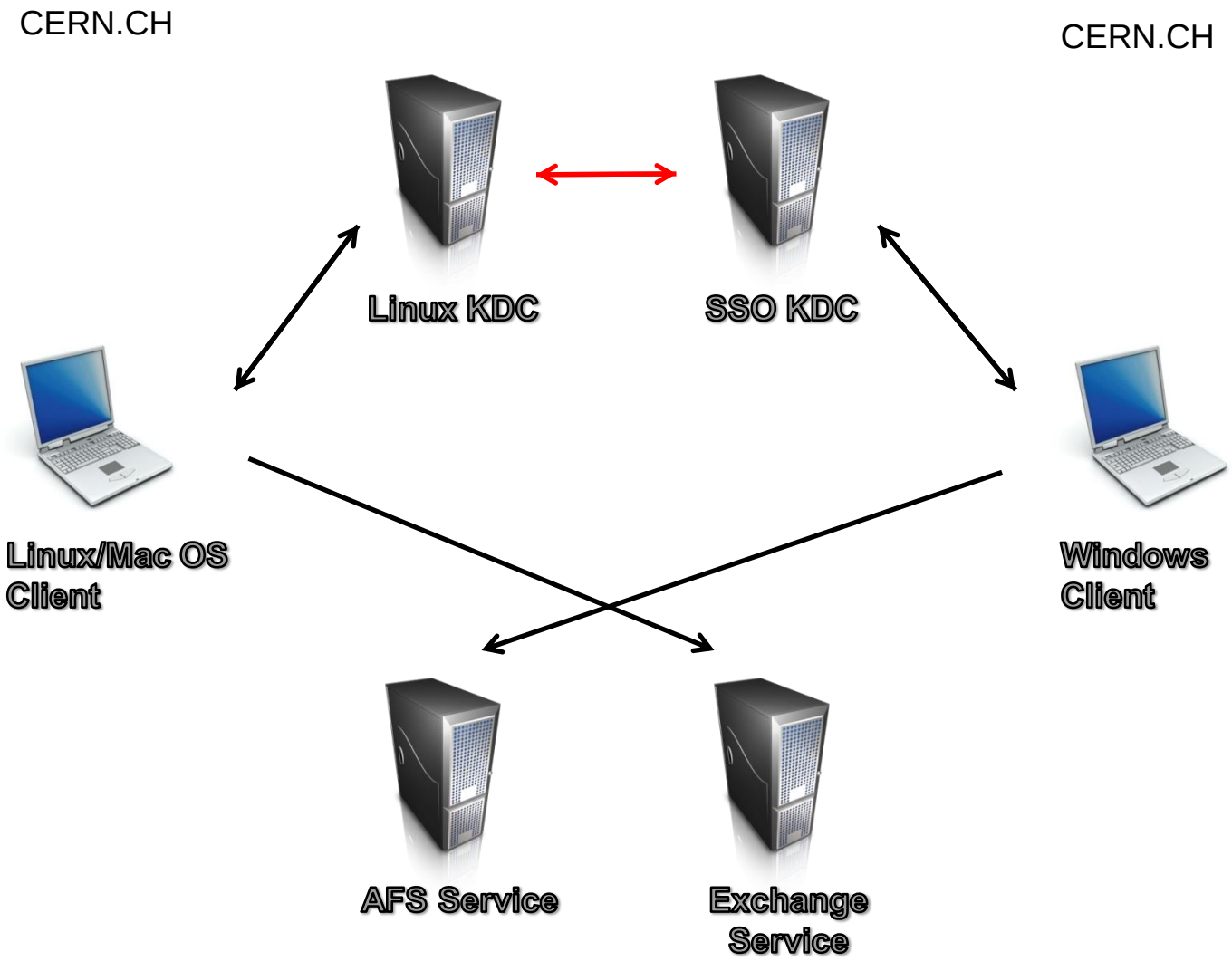
- All areas have undergone extensive testing, which will continue
- The rollout is gradual, no big bang approach
- Documentation and help channels will be put in place

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Questions?

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Alternative Solutions: Trust Relationship



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Alternative Solutions Cont.

CERN IT Department

- **Renaming the Linux realm** would require roughly the same amount of time as a complete migration, but synchronisation/KDC running still remain.
- External users will need to specify the new realm name when authenticating with CERN.
- **Renaming the SSO realm** would involve a large amount of hardware replication and will result in a ‘disjoint namespace’ which may cause problems with both Microsoft and third party software.
- **Migrating to Heimdal** means moving away from a commercially supported solution, which is responsible for CERN’s other authentication mechanisms (certificates/xldap).

- https://twiki.cern.ch/twiki/bin/view/AFSService/UnifiedKerberos for more information on investigation

Migration Cont

- Batch/Acron Impersonation Systems
  - Systems require fresh user credentials for impersonation
  - No direct equivalent to Heimdal ‘key extraction’ approach
  - Nodes will now contact new system based on pkinit or original Heimdal system depending on flavour of node/client to acquire user credentials
- Key Acquisition
  - Two key sets now maintained in default keytab
  - Historical keys included to ensure smoothest possible transition
  - Alternative keytabs available with single flavour if necessary (although key order in krb5.keytab will correspond to config)
  - Software written to construct keys locally without contacting KDC
- Conflicting credentials
  - Users may authenticate/forward credentials to machine of a different default configuration
  - Pam module detects credential encryption and configures environment so things keep working

KDC Load

- Need to match – add more machines or increase speed
- 1000 TGT requests from 8 lxplus machines simultaneously
  - AFS KDC's: 37 seconds
  - Windows DC's: 54 seconds (still ~11,500,000 per day)

Operation	Daily Load	Peak Daily Load	AD Capacity
database lookup	30,000	60,000	
klog/kinit	200,000	240,000	
krb4 kinit / klog.krb	380,000	410,000	
Krb4 failed lookup	8,000	11,000	
Krb5 failed lookup	15,000	19,000	
Batch/acron kinit	380,000	410,000	
Totals	1,215,000	1,400,000	11,500,000