Integrating Linux systems with Active Directory using Open Source Tools

SLAC 2017, Berlin

Thorsten Scherf
Red Hat

Agenda

- Problem statement
- Aspects of integration
- Integration options
- Recommendations

Problem Statement
and
Aspects of Integration

Problem Statement

- For most companies **AD is the central hub** of the user identity management inside the enterprise
- **All systems** that AD users can access (including Linux) **need** (in some way, i.e. directly or indirectly) **to have access to AD** to perform authentication and identity lookups
- In some cases the AD is the **only allowed central authentication server** due to compliance requirements
- In some cases **DNS is tightly controlled** by the Windows side of the enterprise and non Windows systems need to adapt to this

Integration Aspects

Main aspects

- **Identities**
  - Where are my users stored? What properties do they have? How is this data made available to systems and applications? How this data is delivered to the right endpoints? Is it cached and how it is refreshed?
- **Authentication**
  - What credentials do my users use to authenticate? Passwords? Smart Cards? Special devices? Is there SSO? How can the same user access file stores and web applications without requiring re-authentication?

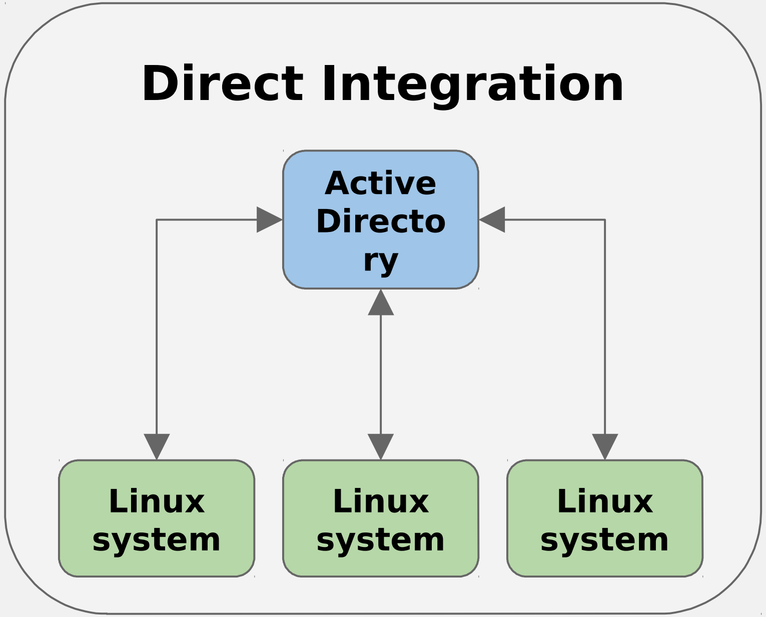
Integration Aspects

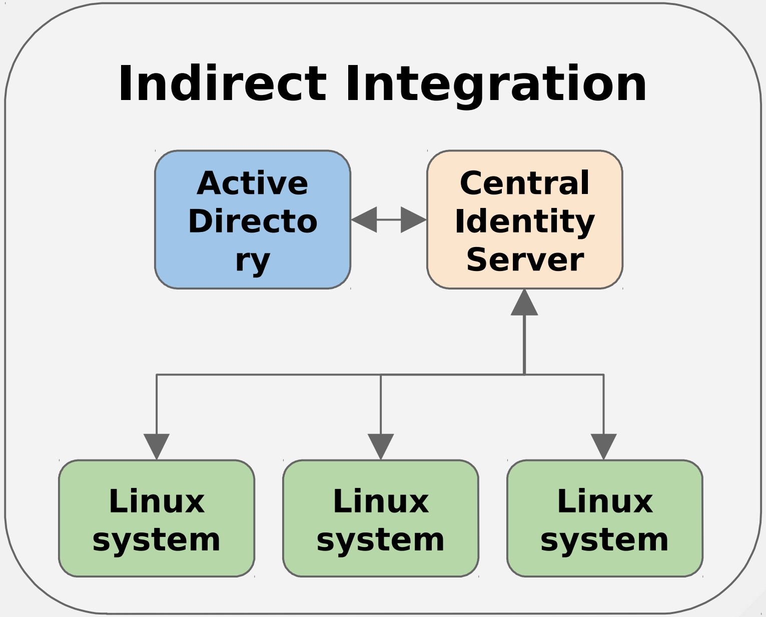
Main aspects, continued

- **Access control**
  - Which users have access to which systems, services, applications? What commands can they run on those systems? What SELinux context is a user mapped to?
- **Policies**
  - What is the type and strength of the credential? What are the SSO ticket/assertion policies? How to express what is allowed and what not in my environment to be compliant with known regulations (PCI, STIG, etc.)?

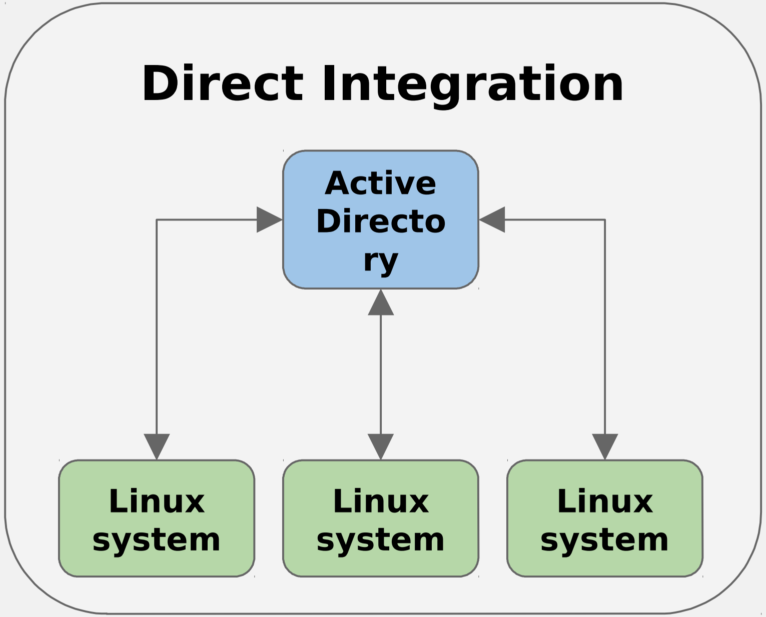
Integration Options

Integration options





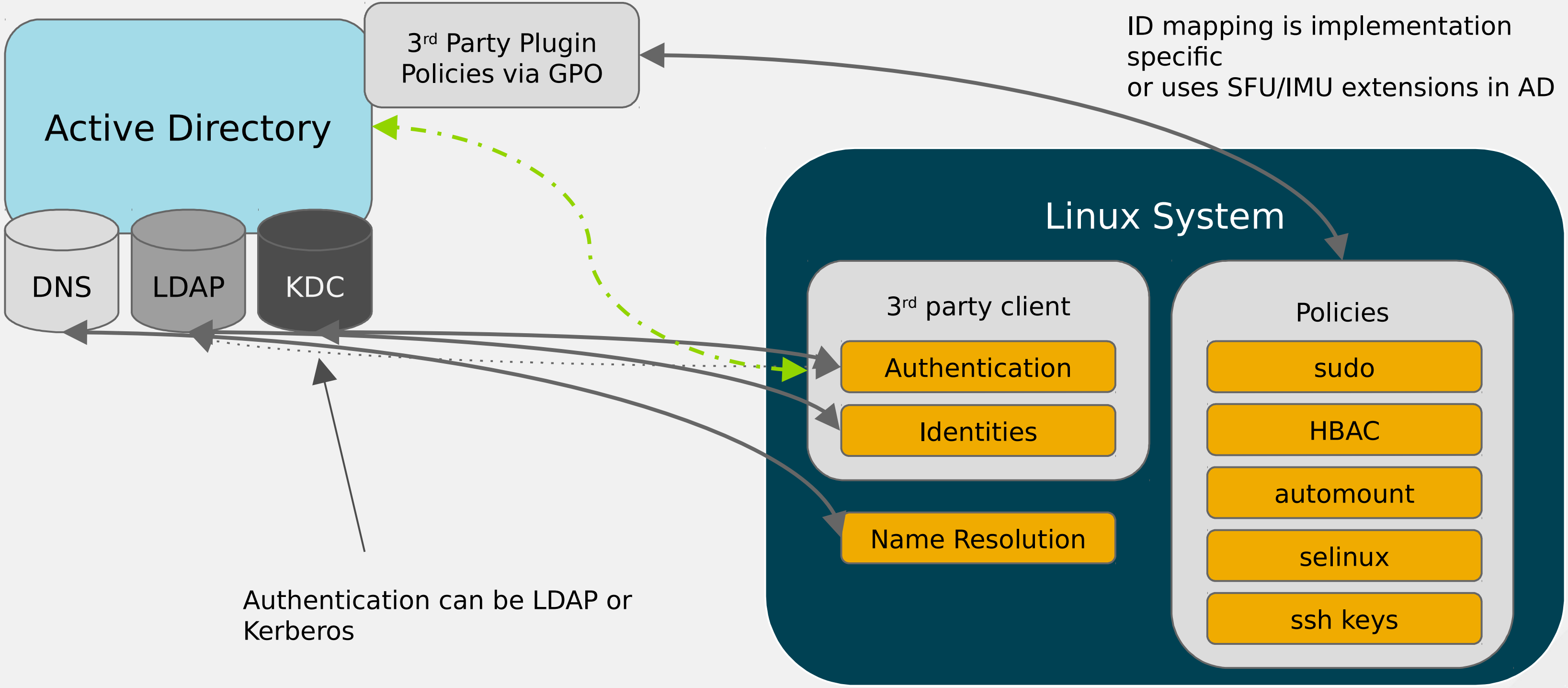
Integration options



Direct Integration Options

- 3rd party
- Legacy (pam_krb5, pam_ldap, nss_ldap, nslcd)
- Traditional – winbind
- Contemporary – SSSD (with realmd/adcli)

Third Party Direct Integration



ID mapping is implementation specific
or uses SFU/IMU extensions in AD

Authentication can be LDAP or Kerberos

Third Party Direct Integration

Pros and Cons

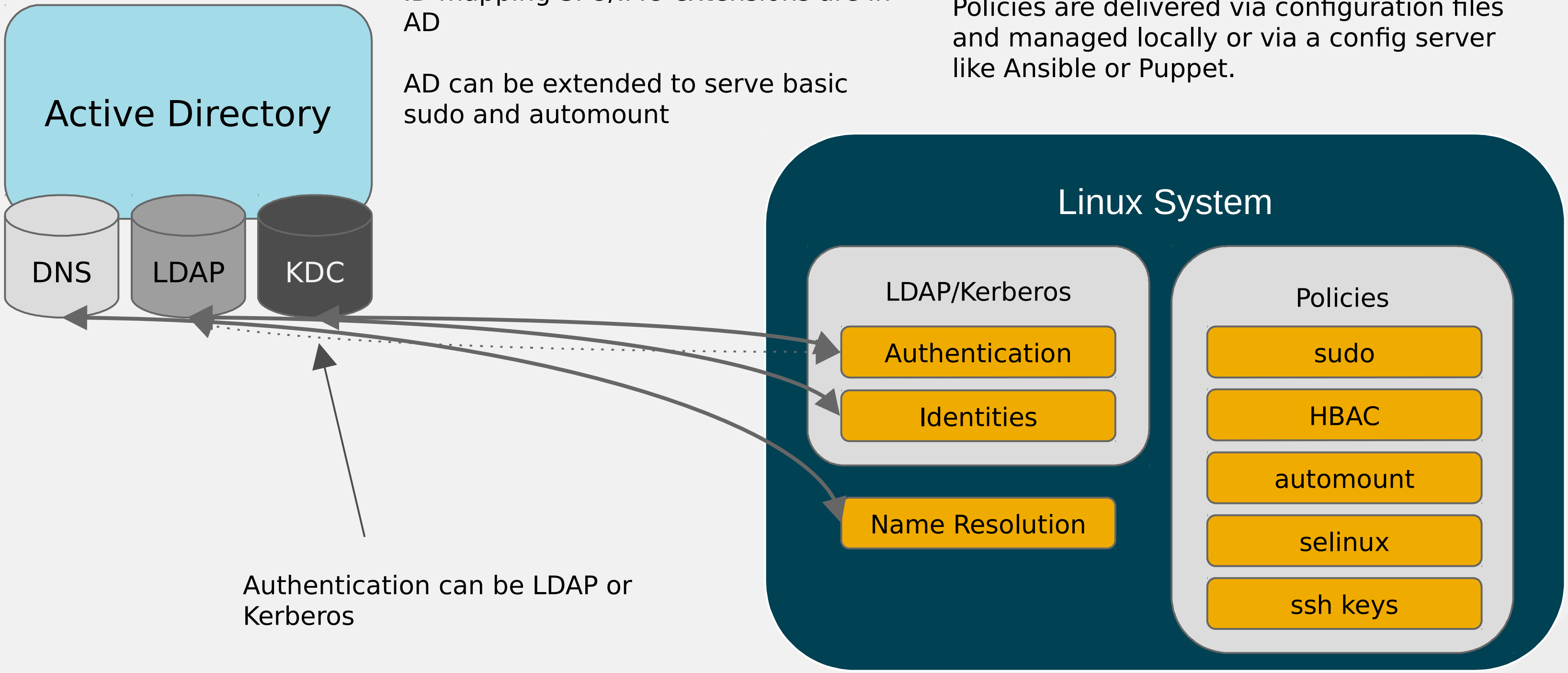
- Pros
  - Everything is managed in one place
  - SSO can be accomplished via Kerberos
- Cons
  - Requires third party vendor
  - Extra cost per system (adds up)
  - Limits UNIX/Linux environment independence
  - Requires software on AD side
  - Policies are not managed or require extra addons

Legacy Direct Integration

ID mapping SFU/IMU extensions are in AD

AD can be extended to serve basic sudo and automount

Policies are delivered via configuration files and managed locally or via a config server like Ansible or Puppet.



Authentication can be LDAP or Kerberos

Legacy Direct Integration

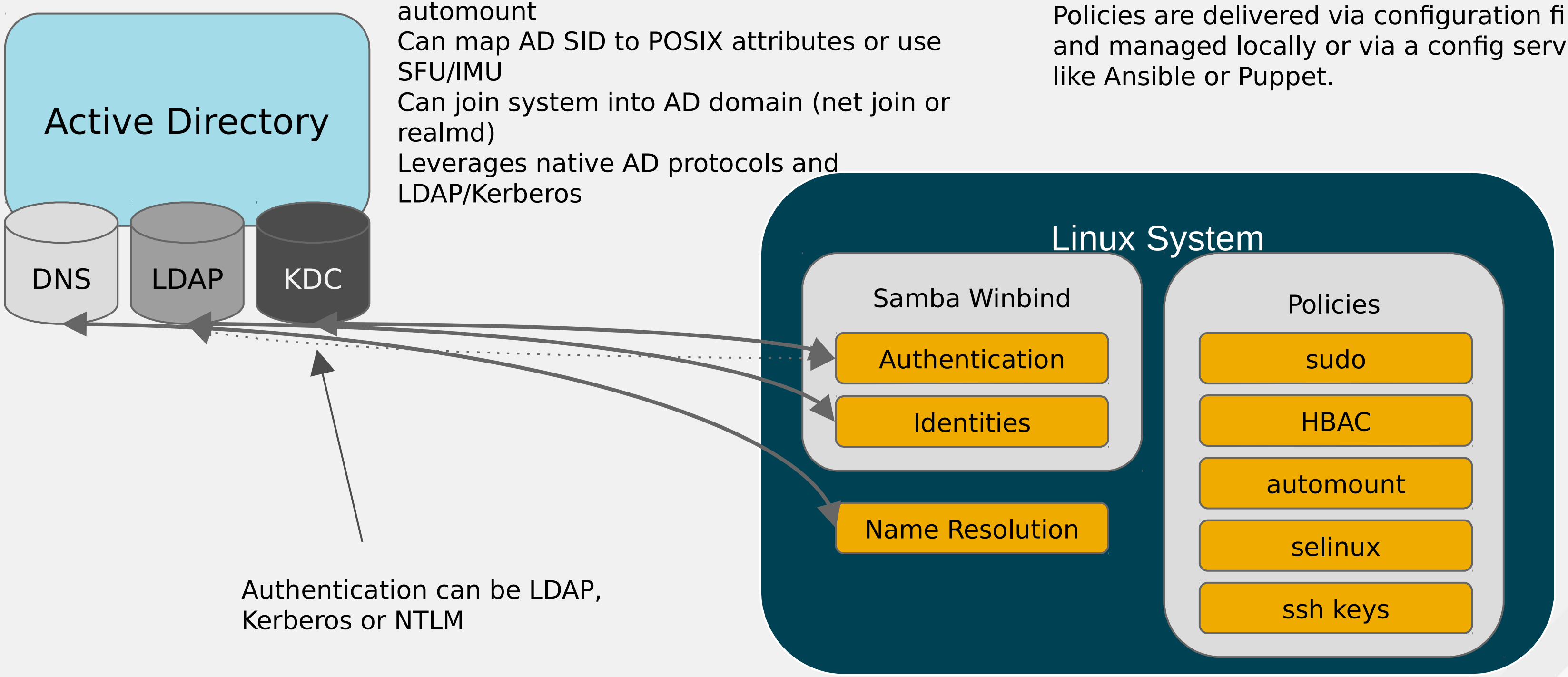
Pros and Cons

- Pros:
  - Free
  - No third party vendor is needed
  - Intuitive
  - LDAP OTP authentication
  - Available on UNIXes
- Cons:
  - Requires SFU/IMU AD extension (already deprecated by Microsoft)
  - Policies are not centrally managed
  - Hard to configure securely
  - No SSO with OTP

Traditional Direct Integration

AD can be extended to serve basic sudo and automount
Can map AD SID to POSIX attributes or use SFU/IMU
Can join system into AD domain (net join or realmd)
Leverages native AD protocols and LDAP/Kerberos

Policies are delivered via configuration files and managed locally or via a config server like Ansible or Puppet.



Authentication can be LDAP, Kerberos or NTLM

Traditional Direct Integration

Pros and Cons

- Pros:
  - Well known
  - Does not require third party
  - Does not require SFU/IMU but can use them
  - Supports trusted forests
  - Supports NTLM fallback
- Cons:
  - Policies are not centrally managed
  - No OTP support

SSSD

Introduction

SSSD = System Security Services Daemon

- SSSD is a service used to retrieve information from a central identity management system.
- SSSD connects a Linux system to a central identity store:
  - Active Directory
  - FreeIPA
  - Any other directory server
- Provides authentication and access control
- Top technology in the evolution chain of the client side IdM components

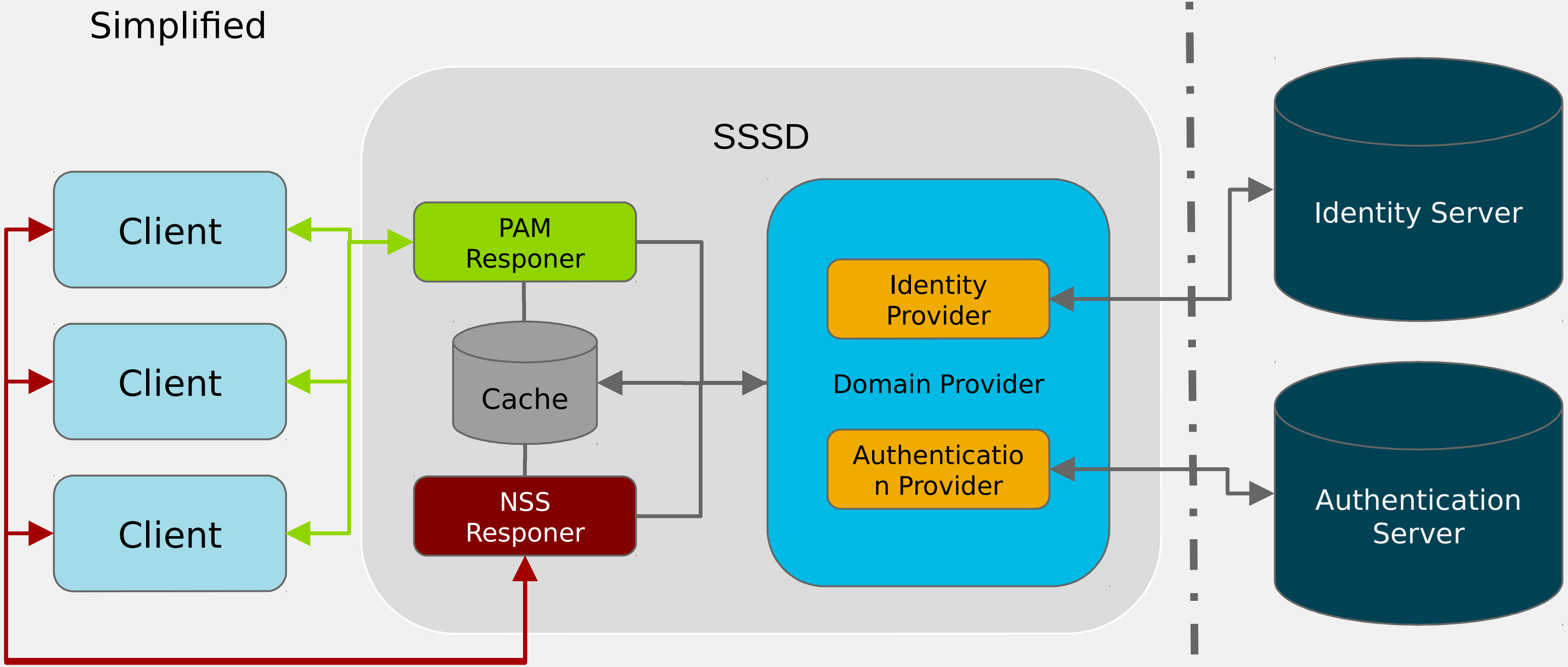
SSSD

Capabilities

- Multiple parallel sources of identity and authentication – domains
- All information is cached locally for offline use
  - Remote data center use case
  - Laptop or branch office system use case
- Advanced features for:
  - FreeIPA integration
  - AD integration

SSSD Architecture

Simplified



Realmd

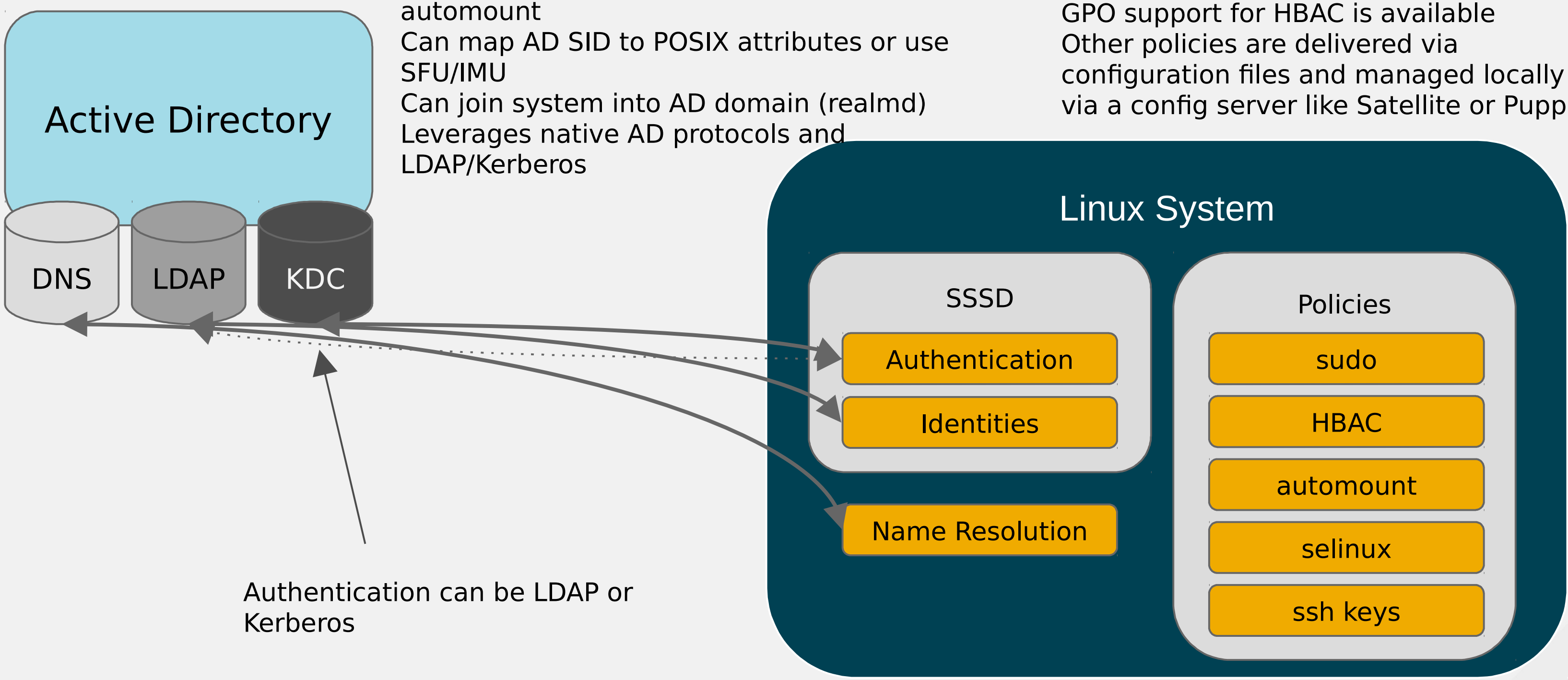
Couple words

- Component of Linux
- Main goal is to detect domain environment using DNS (detection)
  - AD
  - FreeIPA
  - Kerberos
- Join system to the domain (using SSSD or Winbind)
- Do it in one command or click
- Availability: command line, D-BUS interface, system installer, desktop

SSSD Based Direct Integration

AD can be extended to serve basic sudo and automount
Can map AD SID to POSIX attributes or use SFU/IMU
Can join system into AD domain (realmd)
Leverages native AD protocols and LDAP/Kerberos

GPO support for HBAC is available
Other policies are delivered via configuration files and managed locally or via a config server like Satellite or Puppet.



Authentication can be LDAP or Kerberos

SSSD Based Direct Integration

Pros and Cons

- Pros:
  - Does not require SFU/IMU but can use them
  - Can be used with different identity sources
  - Support transitive trusts in AD domains and trusts with FreeIPA
  - Supports CIFS client and Samba FS integration
  - GPO for Windows based HBAC
- Cons:
  - No NTLM support, no support for AD forest trusts
  - No SSO with OTP
  - Not all policies are centrally managed

Direct Integration

Option Summary

- Use SSSD - it provides good enough integration out of box, free and well supported
- Use Winbind if you have special cases when NTLM or cross forest trusts are needed (*)
- Use 3rd party if you want super advanced functionality and have extra money
- Do not use legacy setup

Direct Integration

Issues

- Policy management is still not fully central
- Might require extensions on the AD side
- Per system CALs add to cost
- Linux/UNIX administrators do not have control over the environment

FreeIPA/IdM

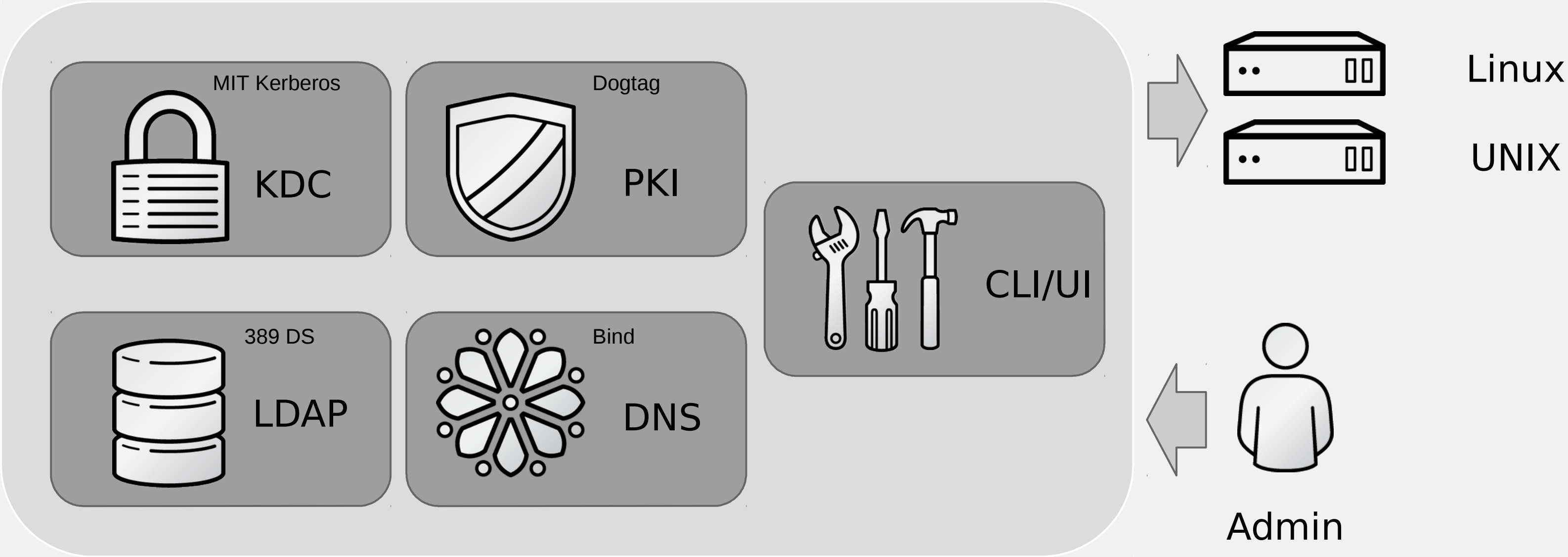
FreeIPA/IdM

Introduction

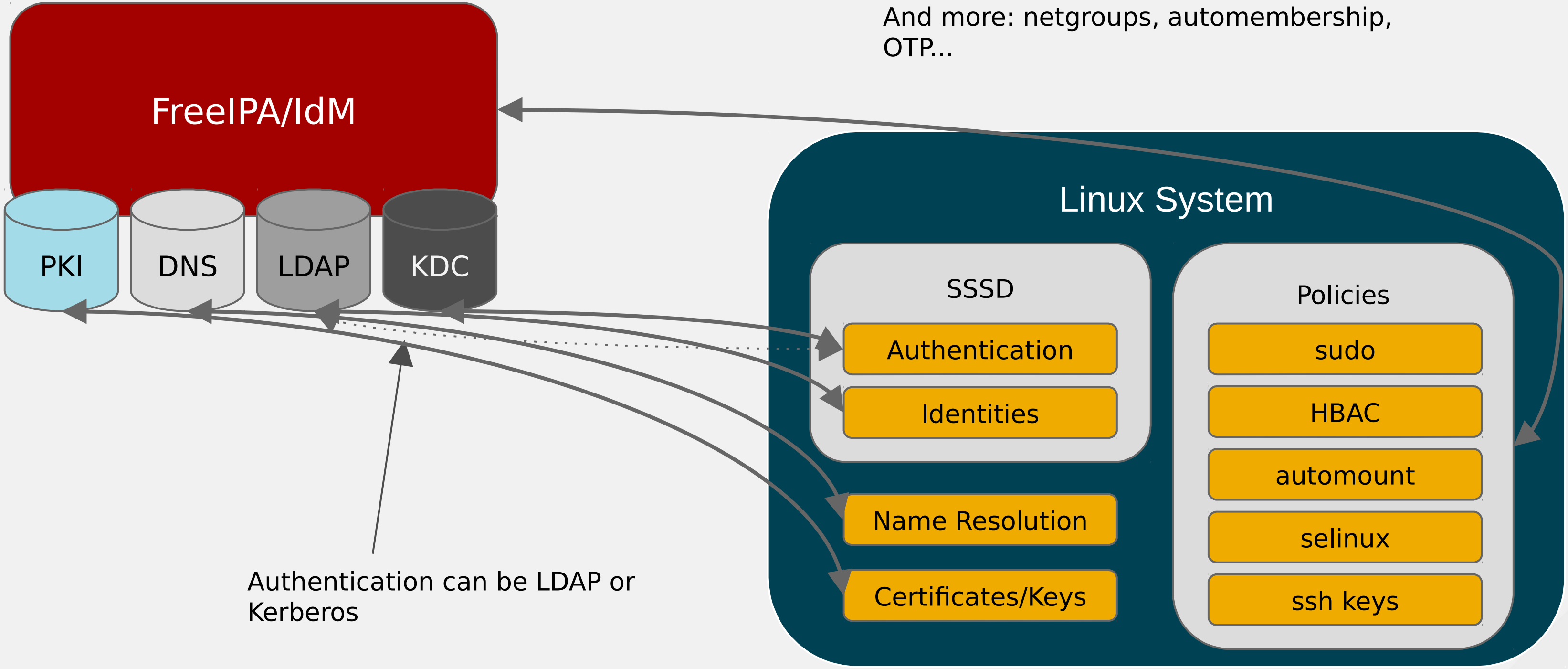
- IdM – Identity Management in Red Hat Enterprise Linux
- Based on FreeIPA open source technology
- IPA stands for Identity, Policy, Audit
  - So far we have focused on identities and related policies
  - Audit is coming but it is bigger than FreeIPA

FreeIPA/IdM

High Level Architecture



FreeIPA/IdM Integration



And more: netgroups, automembership, OTP...

Authentication can be LDAP or Kerberos

FreeIPA/IdM

Features

- Centralized authentication via Kerberos or LDAP
- Identity management:
  - users, groups, hosts, host groups, netgroups, services
  - user lifecycle management
- Manageability:
  - Simple installation scripts for server and client
  - Rich CLI and web-based user interface
  - Pluggable and extensible framework for UI/CLI
  - Flexible delegation and administrative model
    - Self, delegated, role based; read permissions

FreeIPA/IdM

Features Continued

- Host-based access control
- Centrally-managed SUDO
- SSH key management
- Group-based password policies
- Automatic management of private groups
- Can act as NIS server for legacy systems
- Painless password migration
- SELinux user mapping
- Auto-membership for hosts and users
- Serving sets of automount maps to different clients
- Different POSIX data and SSH keys for different sets of hosts

FreeIPA/IdM

Features DNS

- DNS is optional but convenient
- Advantages (automation and security):
    - The SRV records get created automatically
    - Host records get created automatically when hosts are added
    - The clients can update their DNS records in a secure way (GSS-TSIG)
    - The admin can delegate management of the zones to whomever he likes
    - Built in DNSSEC support
- Disadvantages:
    - You need to delegate a zone

FreeIPA/IdM

More Features

- Replication:
  - Supports multi-server deployment based on the multi-master replication (up to 60 replicas)
  - Recommended deployment 2K-3K clients per replica
  - Details depend on the number of data centers and their geo-location
- 2FA
  - Native HOTP/TOTP support with FreeOTP and Yubikey
  - Proxied 2FA authentication over RADIUS for other solutions
  - 2FA for AD users (in works)
- Backup and Restore
- Compatibility with broad set of clients (LINUX/UNIX)

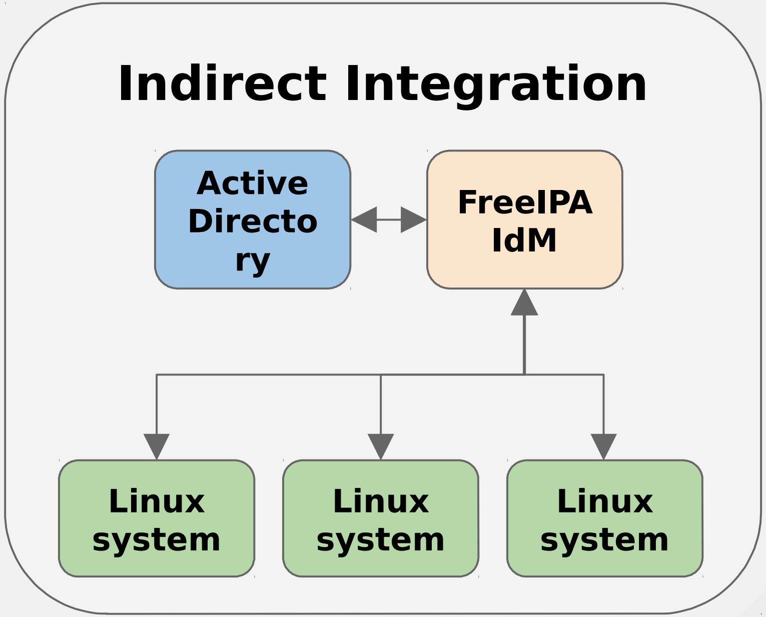
FreeIPA/IdM

Features PKI

- CA related capabilities
  - Certificate provisioning for users (new), hosts and services
  - Multiple certificate profiles
  - Sub CAs
- CA deployment types
  - CA-less
  - Chained to other CA
  - Self signed root
- Tool to change deployment type and rotate CA keys
  - Flexibility in deploying CAs on different replicas
- Key store (Vault)

Indirect Integration using FreeIPA/IdM

Integration options



Integration Paths

Overview

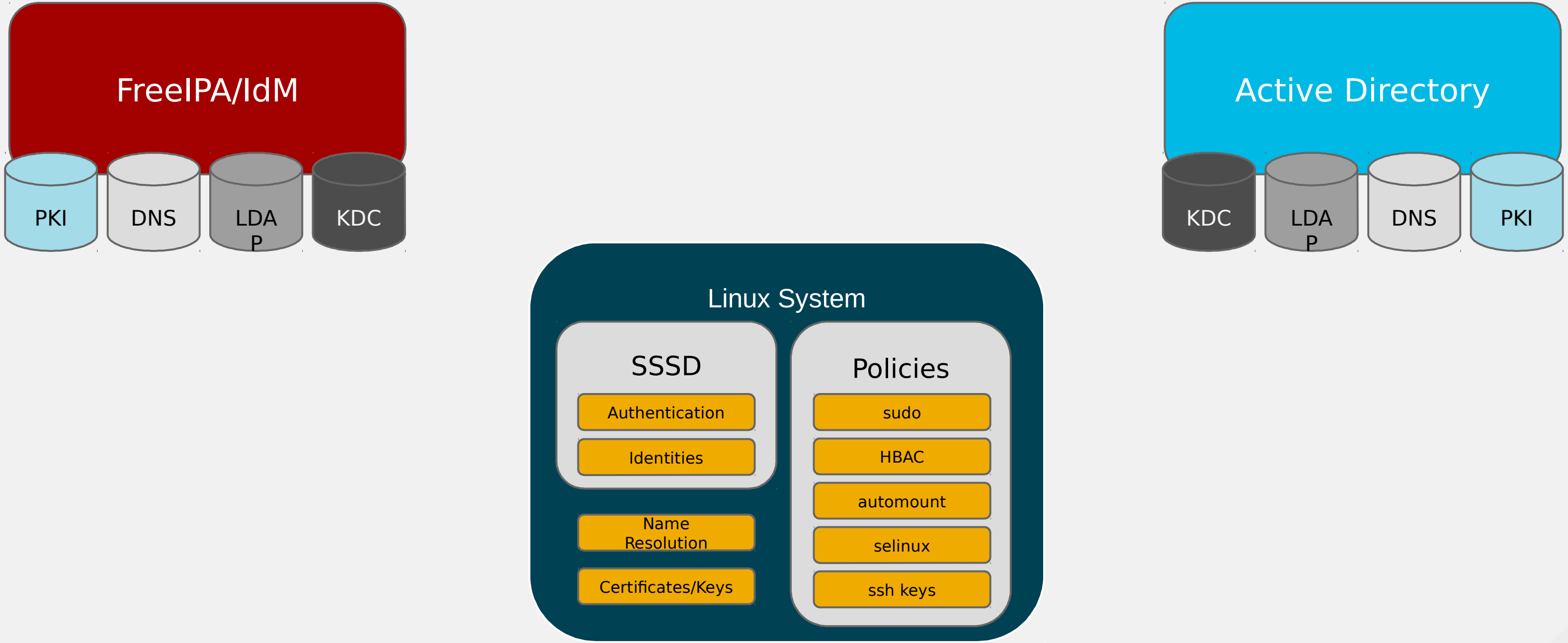
- User and password synchronization (not recommended)
- Cross forest trusts (recommended)

Synchronization Solution

Overview

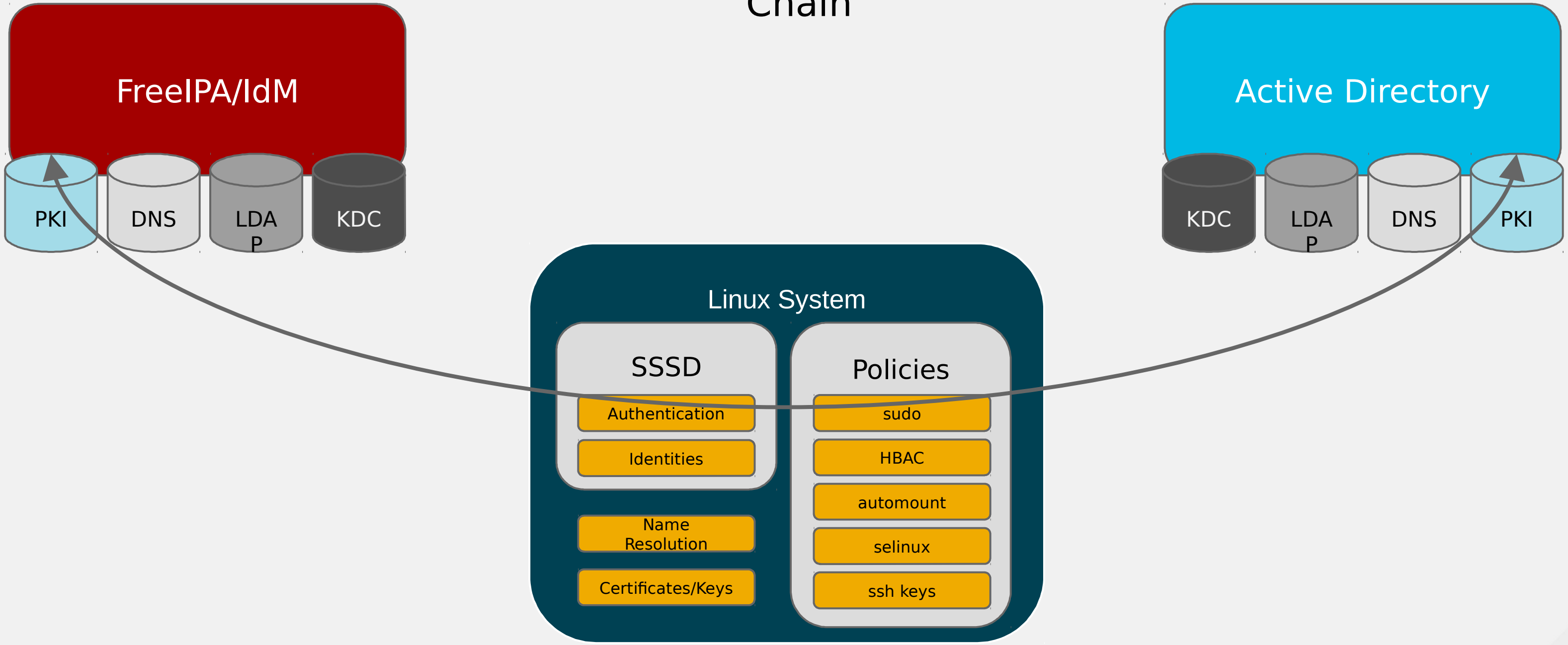
- LDAP level synchronization
- AD is the authoritative source - one way sync
- No group synchronization, only users
- Only one domain can be synchronized
- Single point of failure - sync happens only on one replica
- Limited set of attributes is replicated
- Passwords need to captured and synced
  - Requires a plugin on every AD DC
  - Mismatch of password policies can lead to strange errors

FreeIPA/IdM AD Integration with Trust

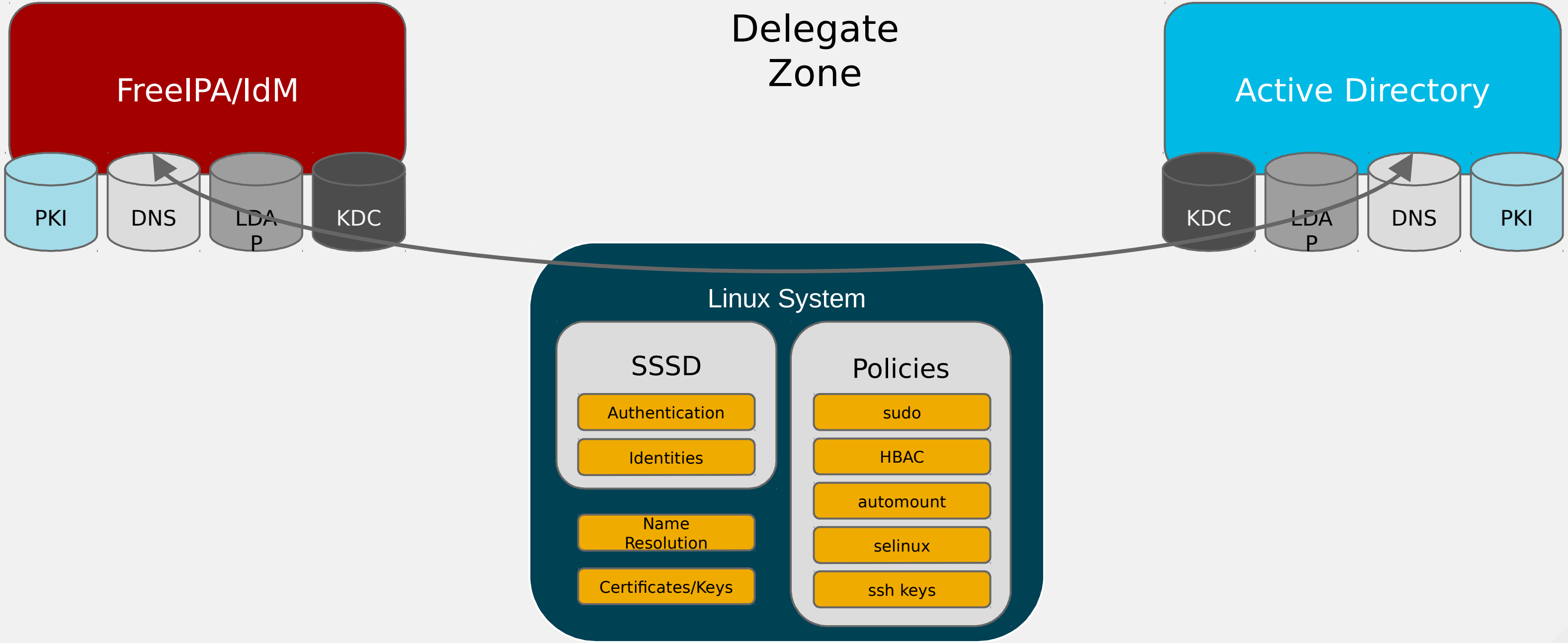


FreeIPA/IdM AD Integration with Trust

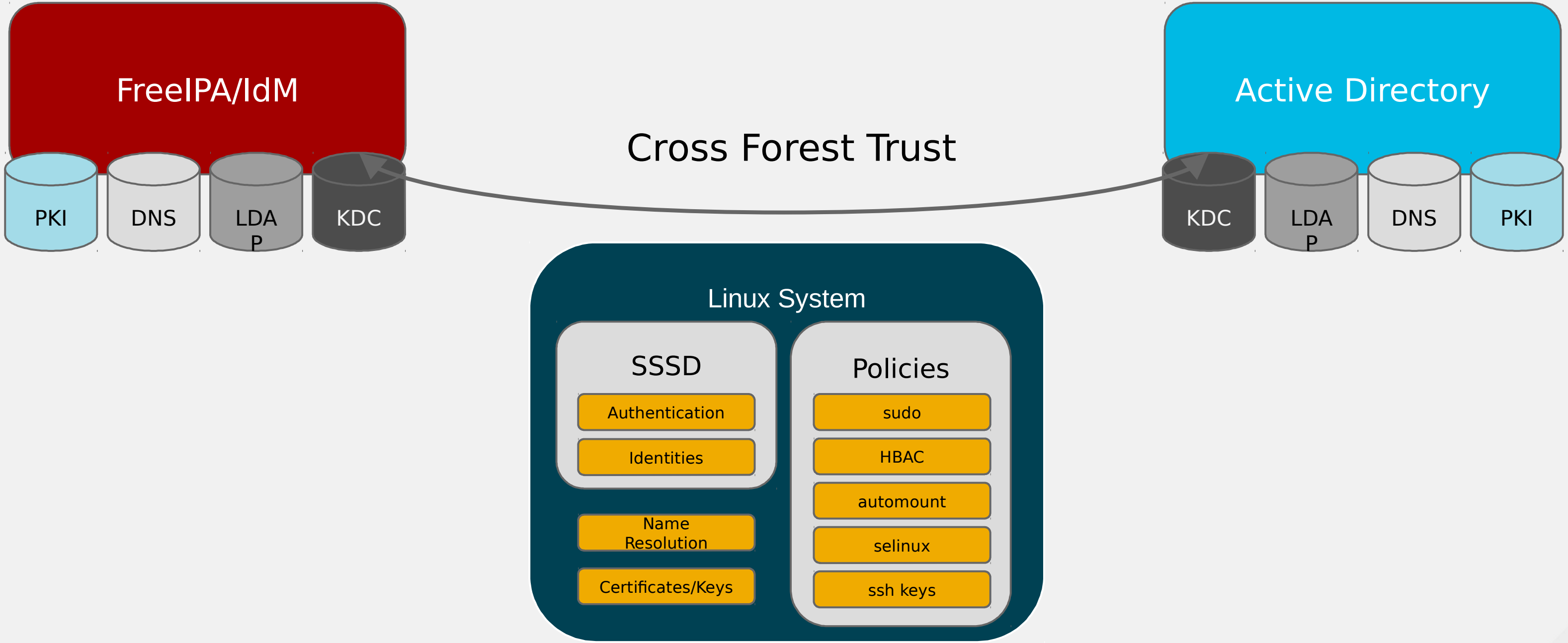
Chain



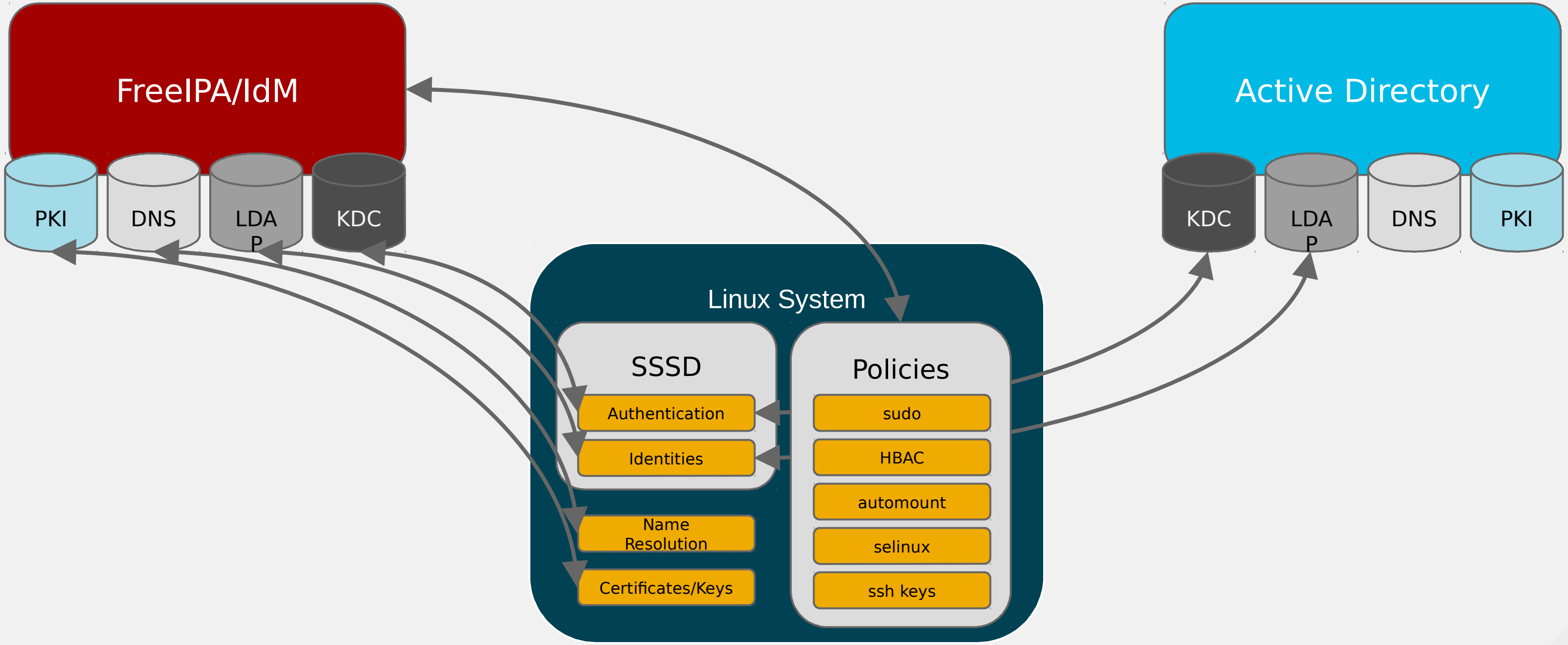
FreeIPA/IdM AD Integration with Trust



FreeIPA/IdM AD Integration with Trust



FreeIPA/IdM AD Integration with Trust



User Mapping

Details

- Can leverage SFU/IMU for POSIX (brown field)
- Can do dynamic mapping of the SIDs to UIDs & GIDs (green field)
- Static override with ID views

Trust

Details

- Two-way and one-way trust (FreeIPA trusts AD)
    - AD/Samba DC trusting FreeIPA is on the roadmap
- Trust agents (different behavior of different replicas)

Trust Based Solution

Pros and Cons

- Pros:
  - Free (FreeIPA/IdM is a part of OS)
  - Reduces cost – no CALs or 3rd party
  - Policies are centrally managed
  - Gives control to Linux admins
  - Enabled independent growth of the Linux environment
  - No synchronization required
  - Authentication happens in AD

Trust Based Solution

Pros and Cons

- Requirement:
  - Proper DNS setup
- Cons:
  - Separate server

Summary

- There are different paths to AD integration: direct or indirect
- SSSD is recommended for direct integration for small environments up to 30-50 systems
- FreeIPA/IdM is recommended for bigger environments where management needs to scale and be automated

Questions?

THANK YOU!