Identity Management Technologies in Red Hat product portfolio

Red Hat Tech Day Belgium 2019

Alexander Bokovoy
Sr. Principal Software Engineer
February 5th, 2019

Introduction

Alexander Bokovoy

- Senior Principal Software Engineer
- Core developer of FreeIPA
- Samba Team member

What is Identity Management?

Let us make sure we understand what we are talking about

Wikipedia Definition

Identity Management - (noun)

“Identity management (IdM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.”

What is Identity Management about?

Setting up context

- **Identities**

  Where are my users stored? What properties do they have? How is this data made available to systems and applications?

- **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?

What is Identity Management about?

Setting up context

- **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 is mapped to?

- **Policies**

  What is the strength of the password? What are the automount rules? What are Kerberos ticket policies?

Goals of the Identity Management

- Authentication, federation and single-sign-on in heterogeneous environments
- Consistent delivery of the identity information throughout infrastructure
- High levels of scalability and automation needed for modern environments
- Credential and key lifecycle management

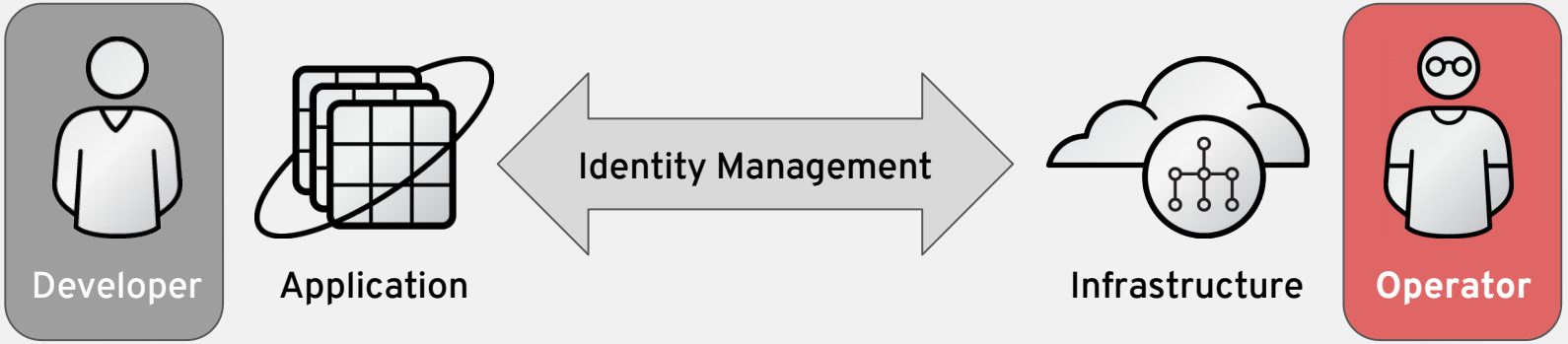
For more details please see Red Hat Summit 2016 presentation (video)

redhat.

Why Identity Management is important?

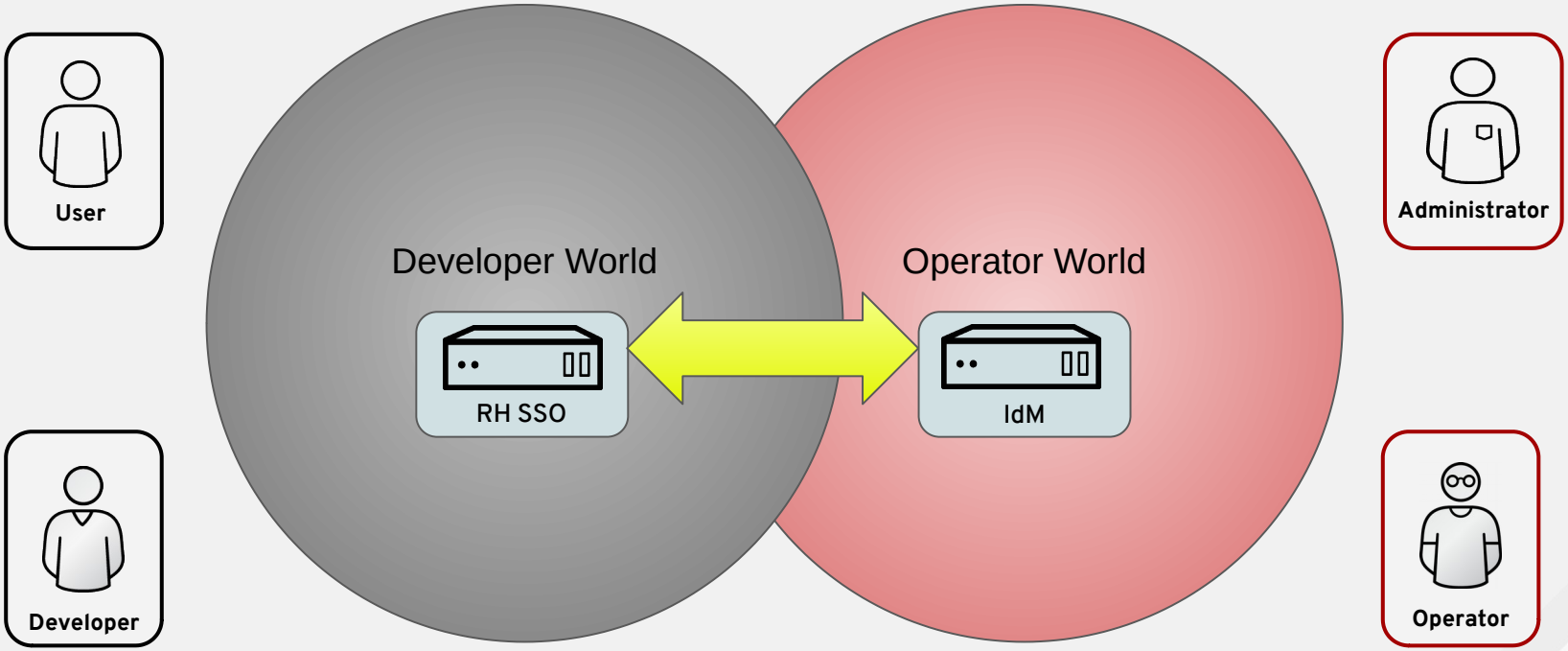
Role of the Identity Management

It is in the middle of everything



Identity Management

Core Components



For more details see [Red Hat Summit 2017 presentation]

Different Worlds Different Needs

Focus of the Core Technologies

- Red Hat SSO
  - Focus on the portfolio integration via SSO
    - Tighter OpenShift integration under way
  - Enables developers to build applications faster offloading authentication woes
- Identity Management in Red Hat Enterprise Linux (IdM)
  - Optimisation of the traditional IT
    - Streamline infrastructure and modernize
    - Automate and scale
    - Reduce costs
    - Improve compliance

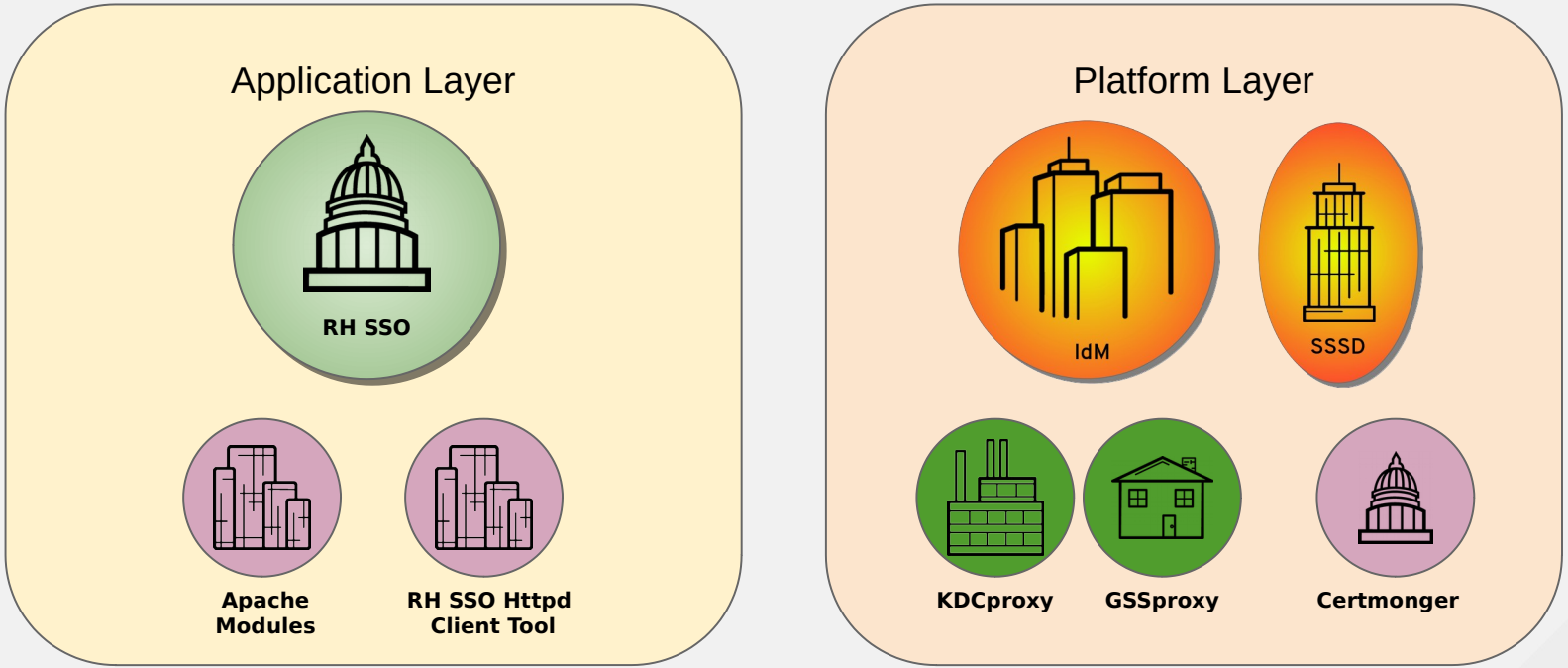
redhat.

Technologies overview

High level overview

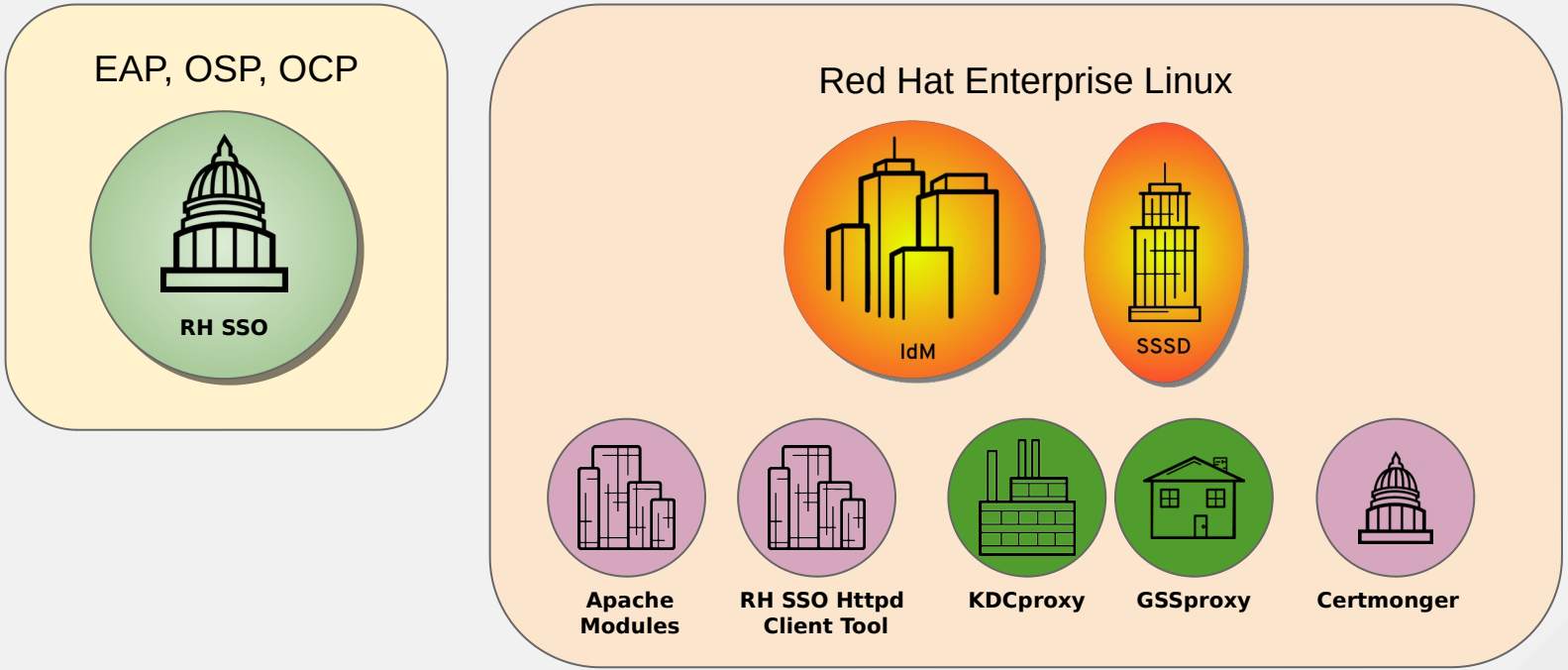
Technologies Layout

Layered view



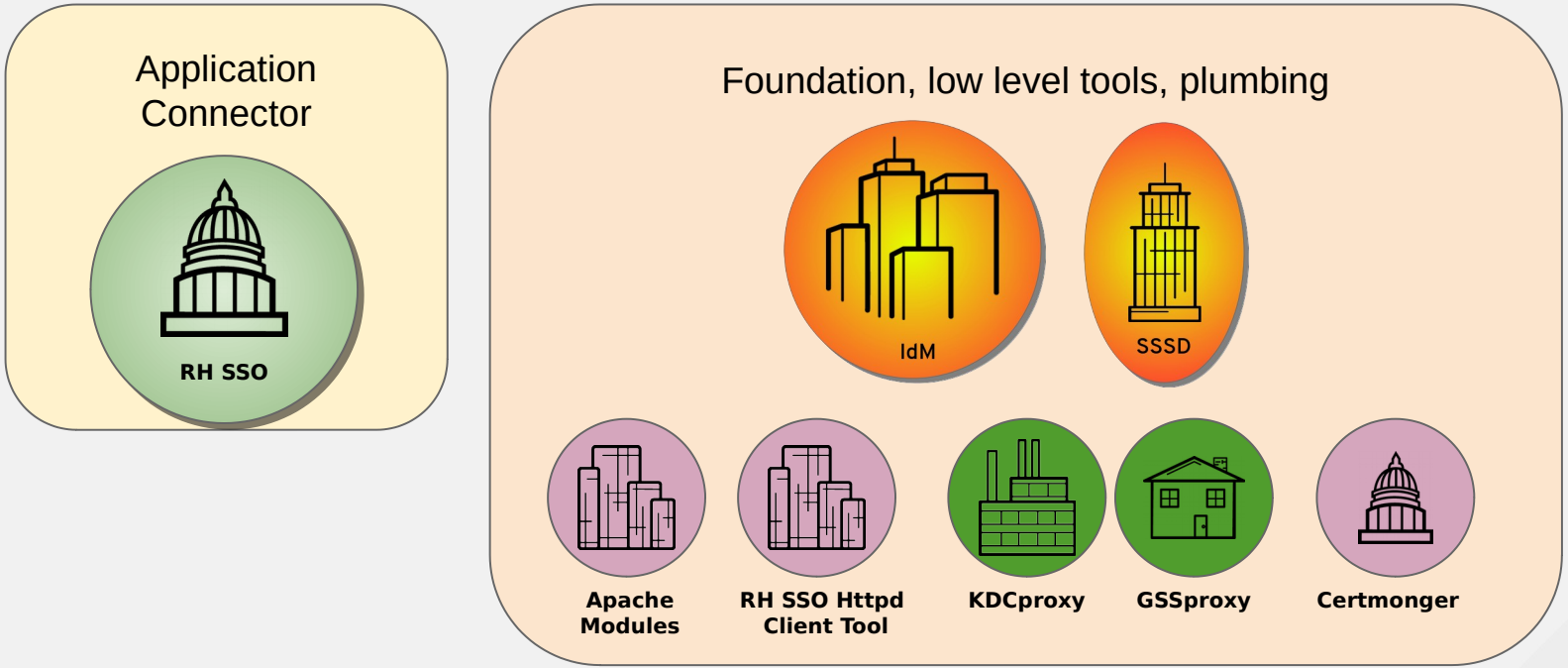
Technologies Layout

Product view



Technologies Layout

Functional view

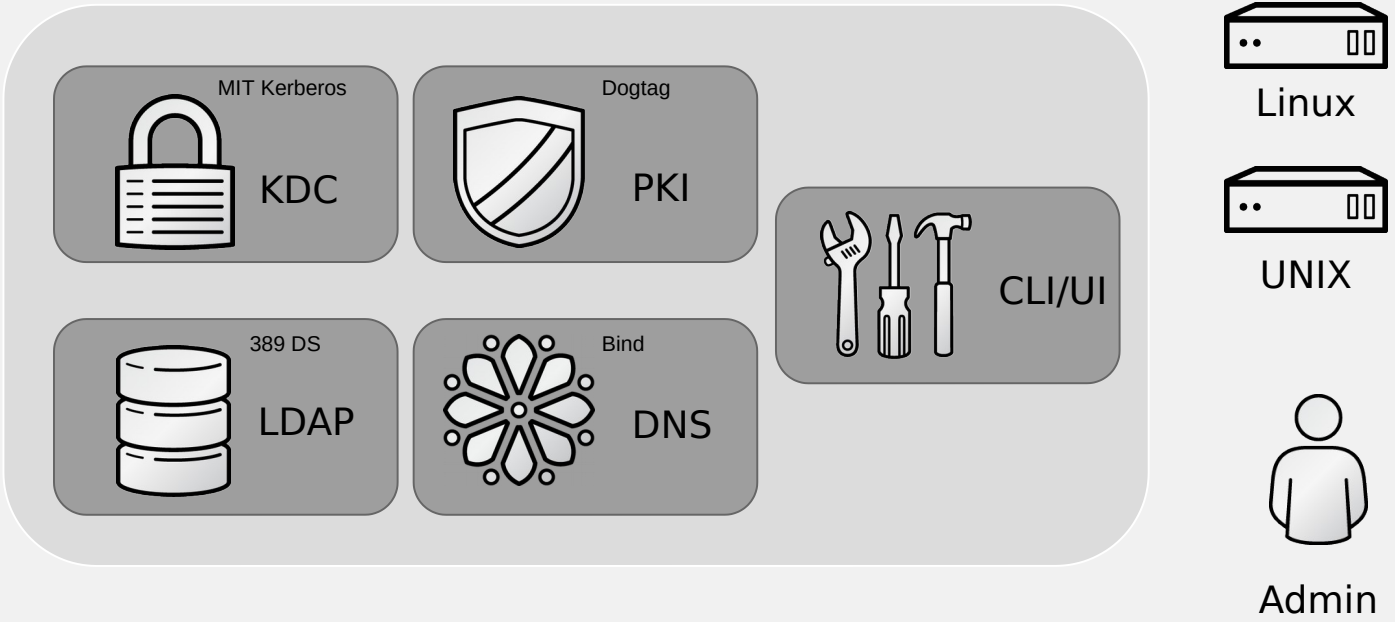


Technologies overview

Dive under the hood

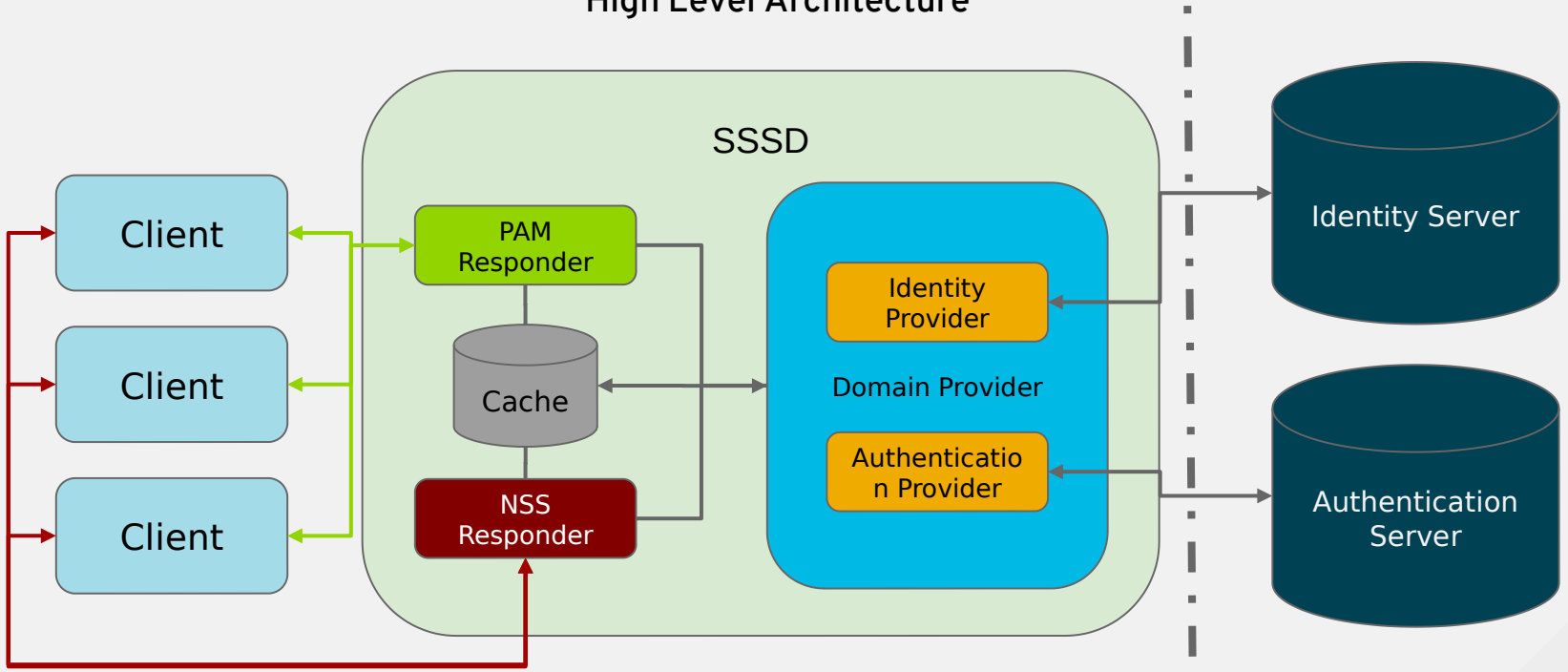
FreeIPA/IdM

High level Architecture

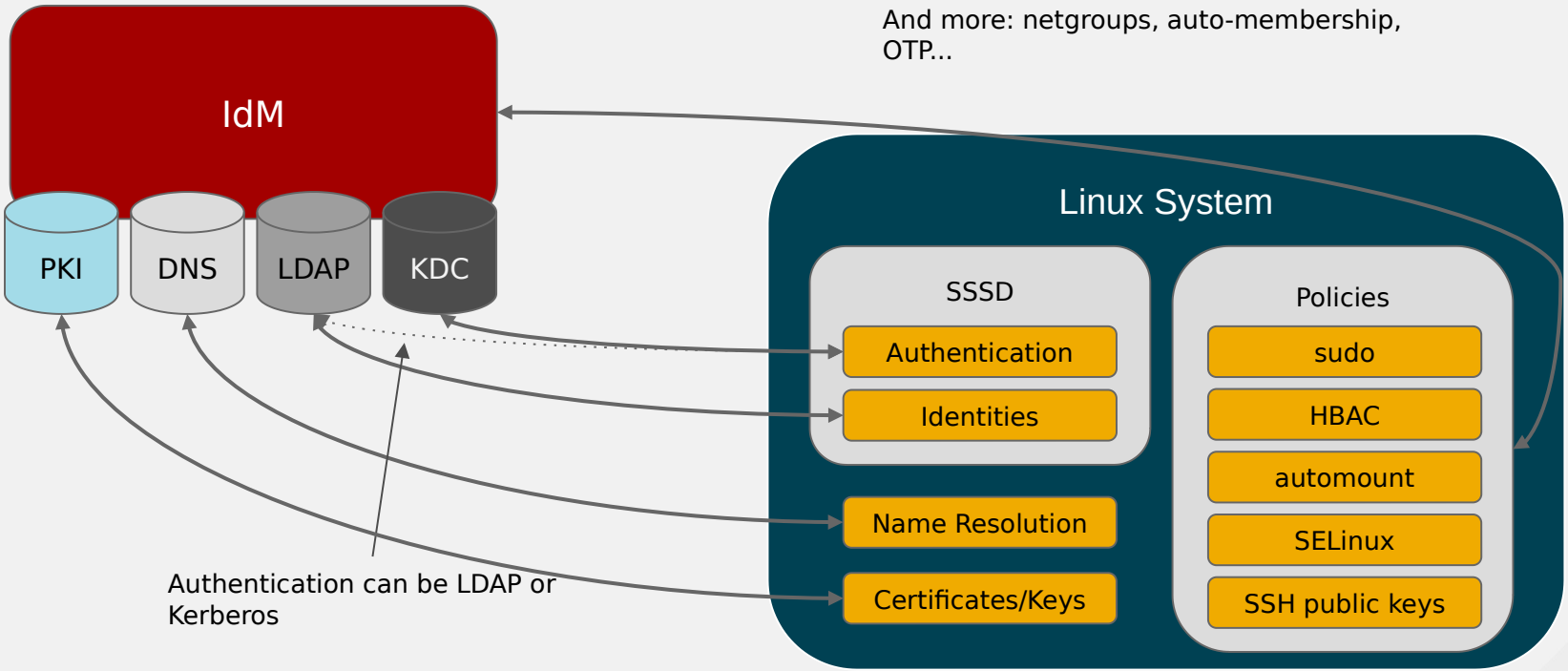


SSSD

High Level Architecture



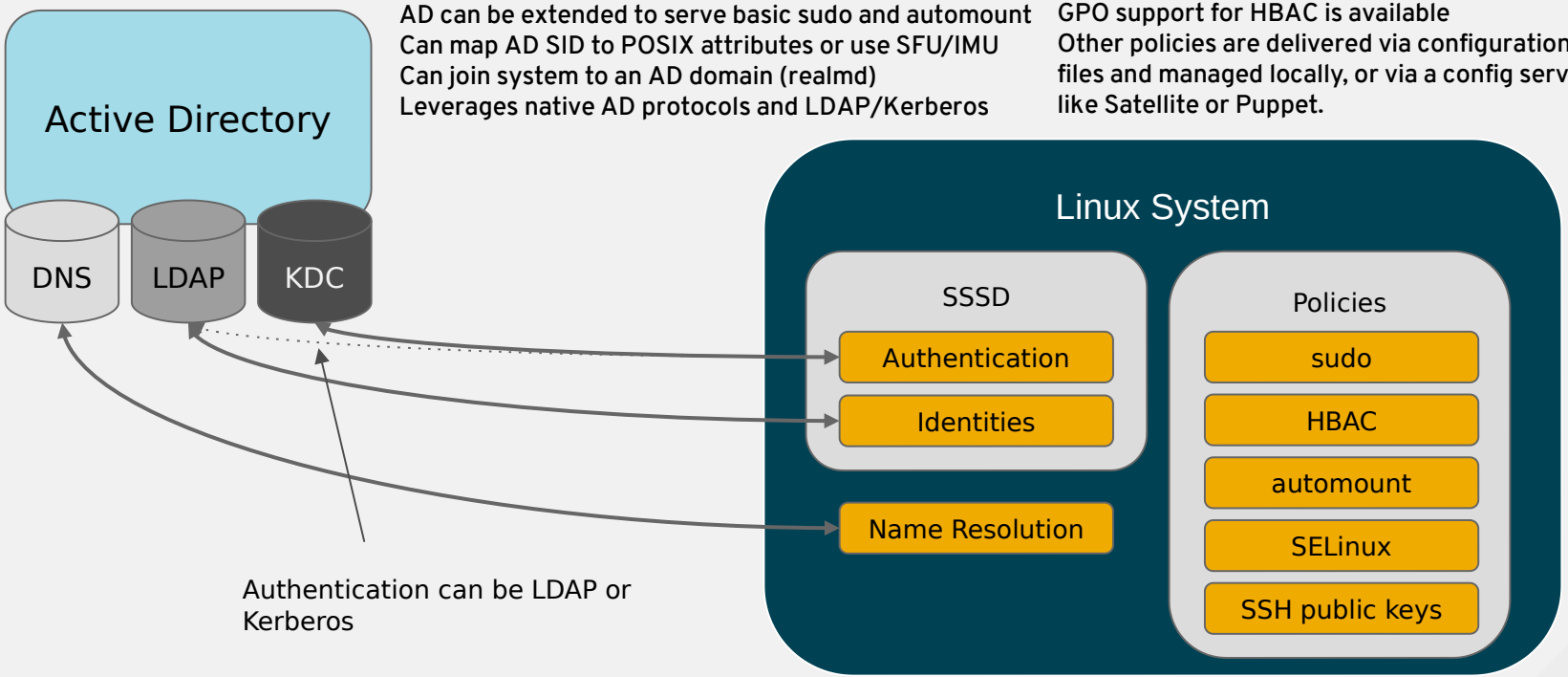
SSSD and IdM Integration



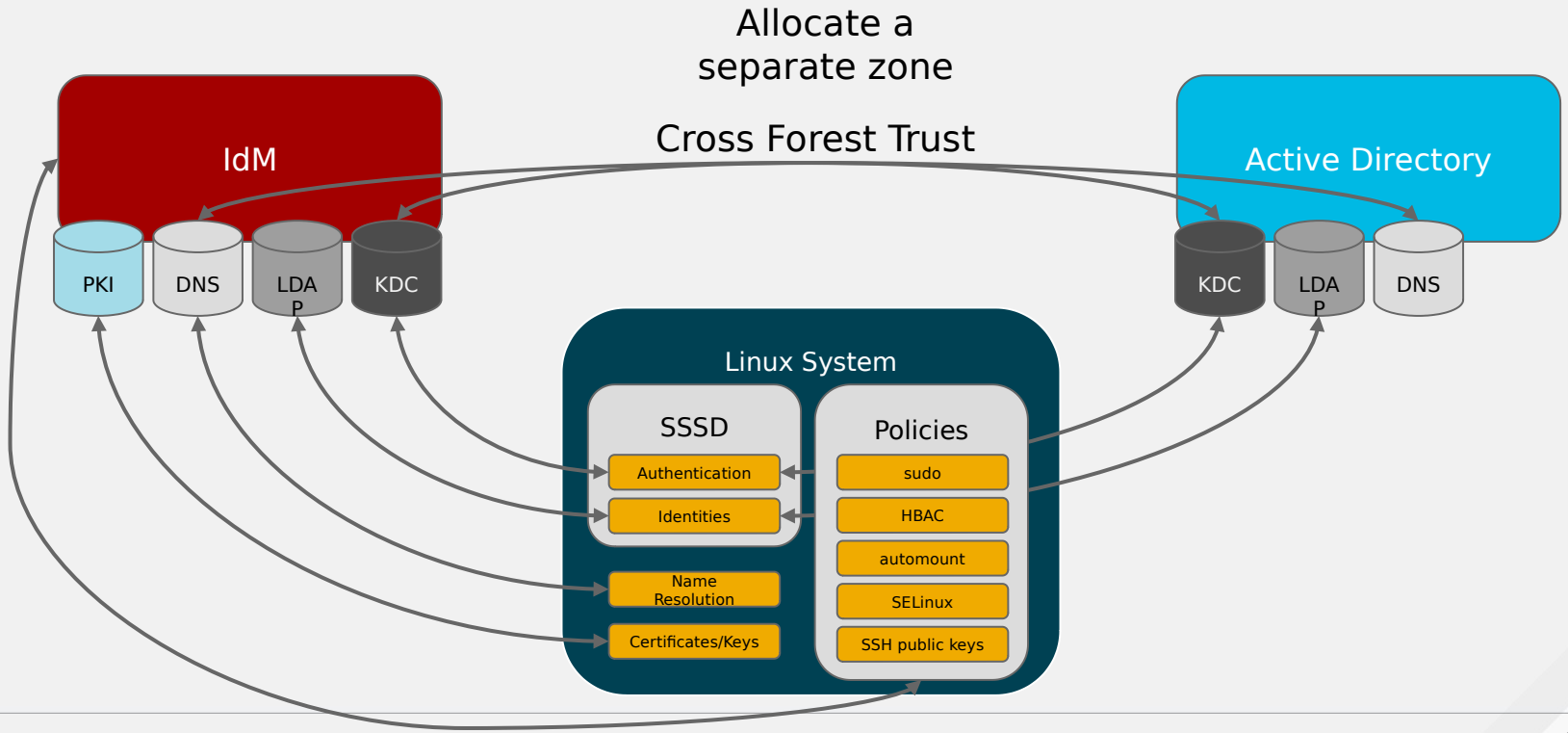
Active Directory and SSSD

AD can be extended to serve basic sudo and automount
Can map AD SID to POSIX attributes or use SFU/IMU
Can join system to an 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.



IdM, SSSD and trust to Active Diretory



Demo

Public demo is provided by FreeIPA project upstream

https://www.freeipa.org/page/Demo

Other technologies

High level overview

- KDCProxy
  - Kerberos traffic over HTTPS through the firewall
  - Useful for DMZ deployments
  - MS-KKDCP protocol
- GSSProxy
  - Reduces attack surface for the network facing services that use Kerberos
  - Kerberos key is inaccessible by the application, allows to enforce privilege separation
  - Automatically renews tickets for application

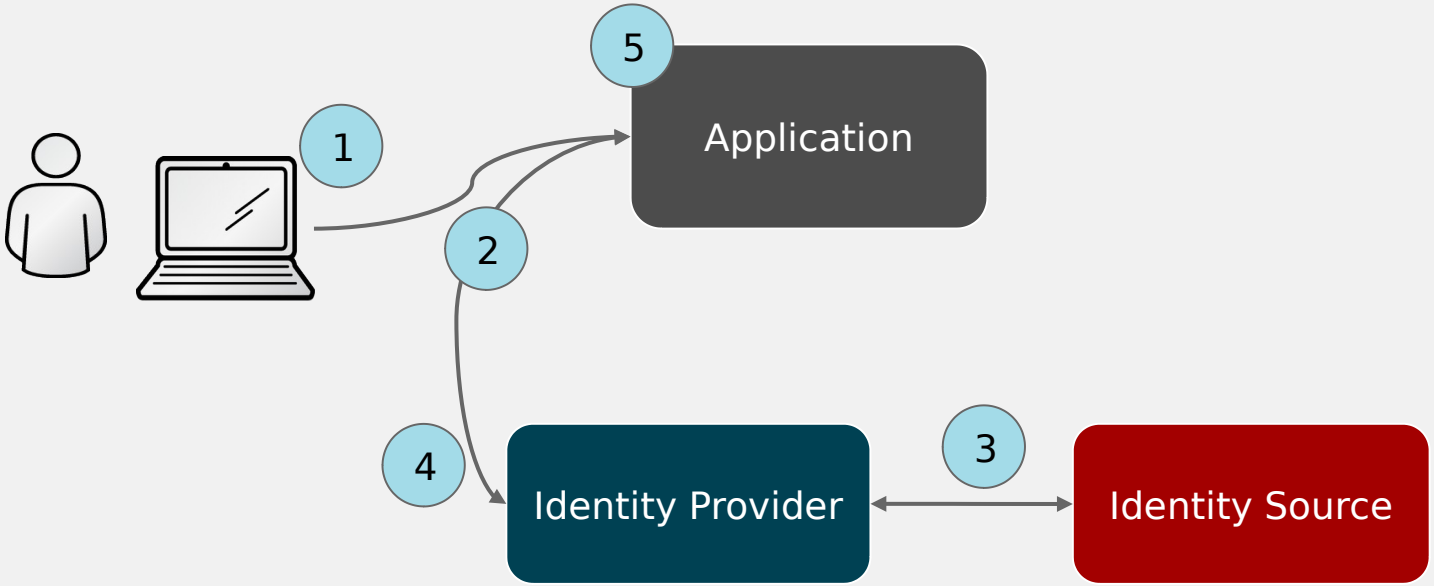
Other technologies

High level overview

- Certmonger
  - Fetch certificates from IdM, track and renew them
  - Useful for automation of the certificate provisioning
  - Red Hat OpenStack Platform uses it to bootstrap its PKI infra

Single sign-on (SSO) Workflow

Simple SAML workflow



Single Sign-On Workflow

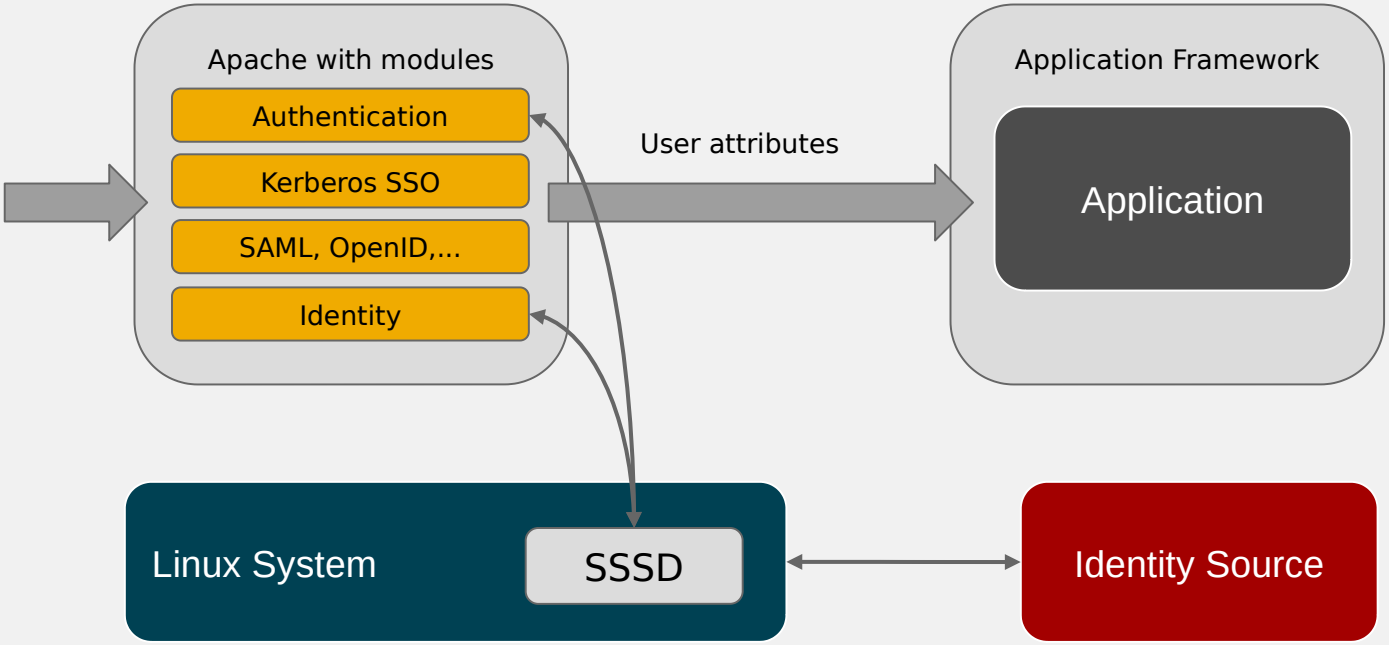
- User starts a browser and navigates to a resource or an application
- Application (Service Provider, SP) checks presence of a valid assertion/token and redirects to the IdP otherwise
- The IdP prompts the user for authentication (or uses SSO) as necessary
- The IdP uses the configured identity source to perform the authentication
- The IdP creates an assertion or token and redirects the browser back to the resource
- Application checks the assertion/token and extracts user data from it
- User is authenticated
- User data is used by the application (for example, for access control decisions)

Red Hat SSO

- RH SSO = Identity Provider (IdP)
- SAML/OpenID Connect protocols
- Easy to use integration libraries and adapters for different application frameworks
- Easy to configure and manage via UI/CLI and REST API
- Centralized session management (easy session termination, single logout)
- User, Role and Authorization Policies management
- Authentication and Registration for end users
- User self service
- RBAC and ABAC with flexible policies
  - With RHEL IdM as a backend for authentication and identity source

Apache Modules

High level overview



Apache Modules

By Function

Authentication Method	Authentication	Access check	Extra user info
Kerberos	mod_auth_gssapi (mod_auth_kerb)	mod_authnz_pam	mod_lookup_idenity
Certificate	mod_ssl		
Formas based	mod_intercept_form_submit		
SAML	mod_auth_mellon		
OpenID Connect	mod_auth_openidc		

Red Hat SSO Httpd Client Tool

- Utility: keycloak-httpd-client-instal
- Command line tool to configure Apache httpd based service providers to be a part of the RH SSO solution
- Supports SAMLv2
- OIDC integration has been prototyped, more work is needed
- What does it do?
  - Connects to RH SSO and registers a service provider
  - Exchanges SAMLv2 metadata with RH SSO (including certificates)
  - Applies configuration to httpd and mod_auth_mellon

Demo

Let us do it!

https://ipa.demo1.freeipa.org

References

Pointers

Useful Links

- Documentation
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/#category-identity-management
  - https://access.redhat.com/documentation/en/red-hat-single-sign-on/
- Demo
  - http://www.freeipa.org/page/Demo
- Blogs
  - http://planet.freeipa.org/
- New training course - RH362 Identity Management

Questions?

redhat®