MIT Kerberos & Red Hat

Past, Present and Future

Dmitri Pal

Sr. Engineering Manager, Red Hat Inc.

October 2012

Agenda

- MIT Kerberos and Red Hat involvement
- Project details
- Future plans

Context

- Red Hat has been a member of the MIT Kerberos consortium for several years
- Red Hat has been contributing code and working closely with MIT development team to deliver features that make Kerberos in Linux environment more relevant for the customers
- Red Hat will continue on this path working on new features for MIT Kerberos in releases to come

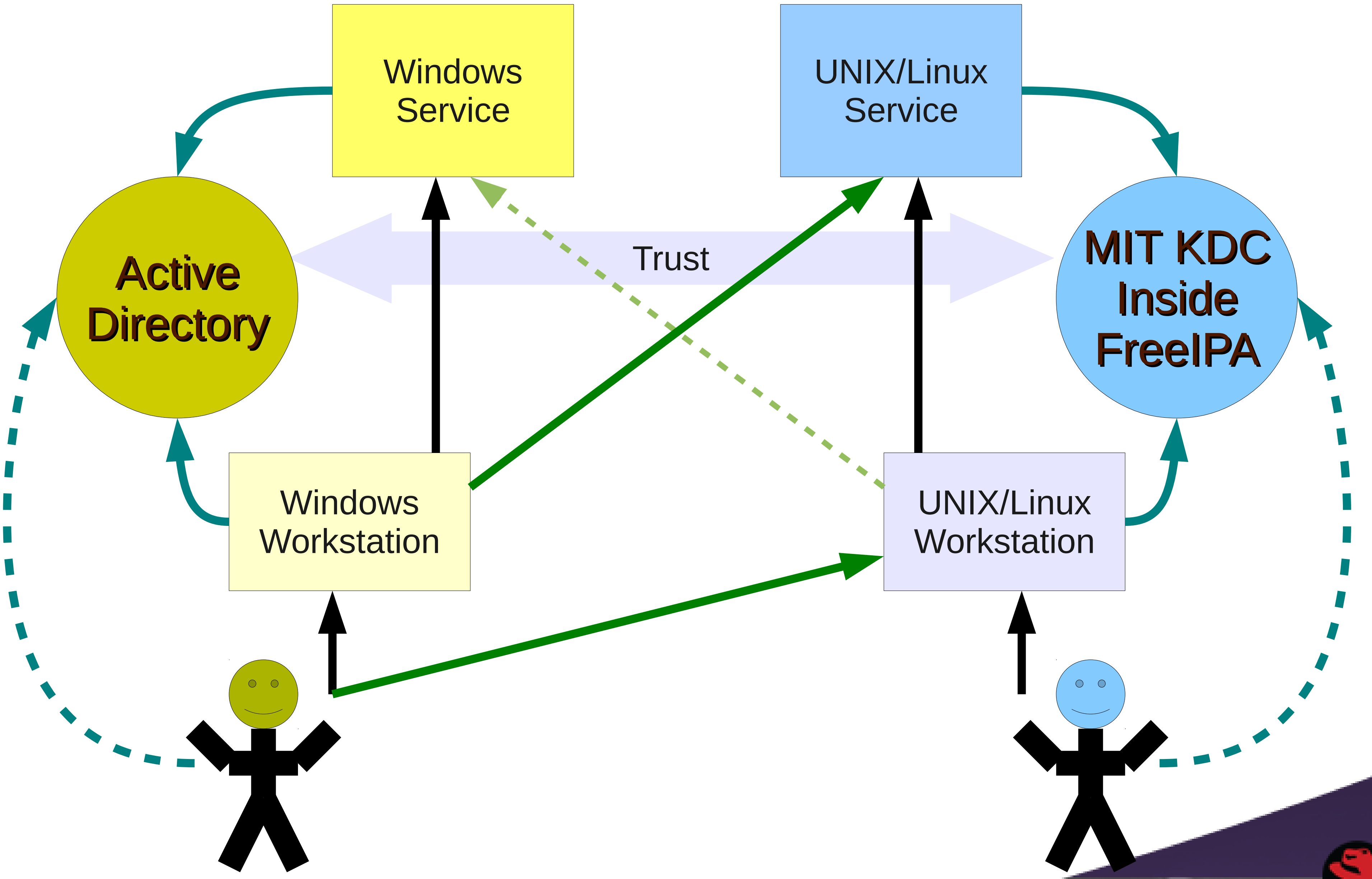
Projects Red Hat is Involved in

- FreeIPA – domain controller for UNIX/Linux
- AuthHub – integrated OTP authentication
- Linux Desktop – improved user experience
- GSS Proxy – better ticket management in GSSAPI
- Key rotation – update keys periodically
- Ticket cache type and location
- Smart card support
- Authorization

FreeIPA Since Last Year

- Released FreeIPA 2.1 under name “Identity Management (IdM) in Red Hat Enterprise Linux” as a part of RHEL 6.2 release in December 2011
- Released FreeIPA 2.2 upstream – May 2012
- Released refresh for IdM based on FreeIPA 2.2 in RHEL 6.3 in June 2012
- Released FreeIPA 3.0 upstream – October 2012
- On the path to deliver FreeIPA 3.0 in RHEL 6.4 in early 2013
  - Main feature – cross realm Kerberos trusts with AD

Cross Realm Kerberos Trust with AD



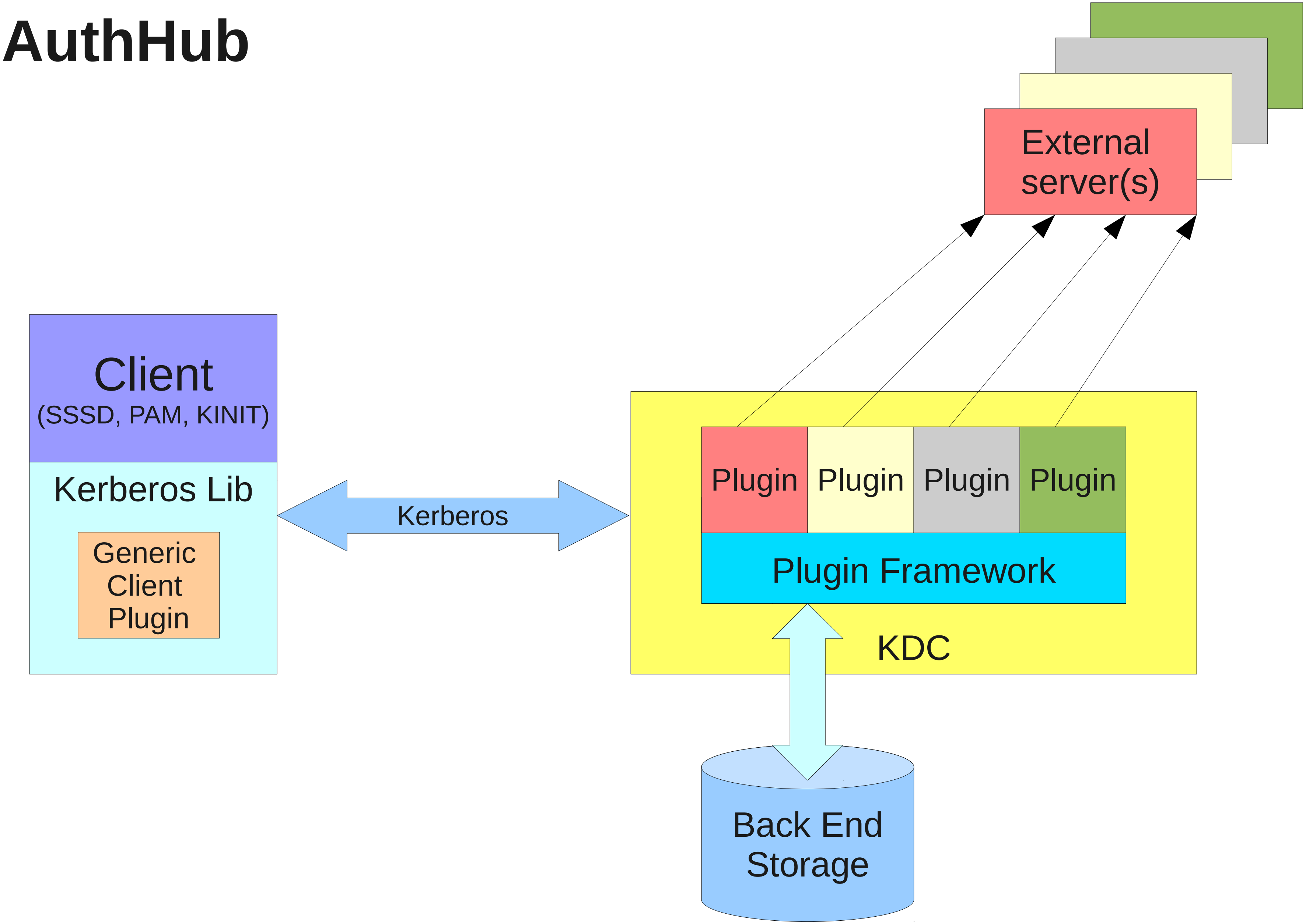
FreeIPA – Next steps

- Pluggable interface for domain - realm lookups
- Pluggable interface to map principal to users
- Case insensitive names/principals for AD compatibility

AuthHub

- https://fedorahosted.org/AuthHub/
- Goal:
  - Make Kerberos KDC pluggable for external authentication methods
- Based on the OTP FAST spec from Gareth Richards
  - https://datatracker.ietf.org/doc/draft-ietf-krb-wg-otp-preauth/
  - In active review

AuthHub


External server(s)
Client
(SSSD, PAM, KINIT)
Kerberos Lib
Generic Client Plugin
Kerberos
Plugin
Plugin
Plugin
Plugin
Plugin Framework
KDC
Back End Storage

AuthHub

- Authentication providers
  - External
    - RADIUS based
    - Yubikey
  - Internal
    - TOTP based (Google authenticator)
    - HOTP based
- Responder API instead of prompter API
  - Slow progress due to complexity of workflows
  - PKINIT is not integrated with new API

AuthHub – Next Steps

- PKINIT integration with responder API
- Switch to using responder API in Fedora
- Async KDB – do not block on the DB lookups
- FreeIPA integration with AuthHub as configuration information storage

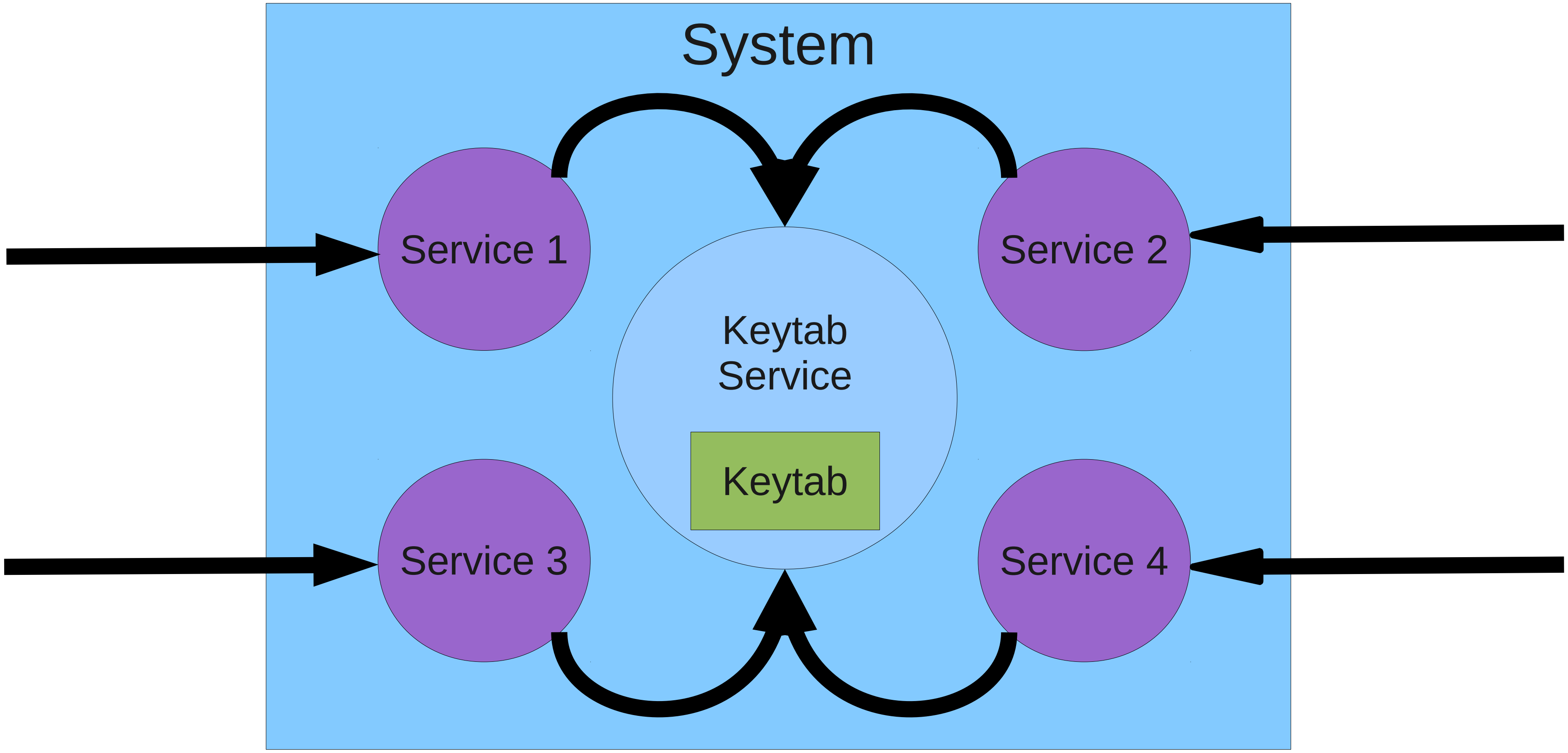
Linux Desktop Integration

- Which credential was used to acquire the ticket?
  - Now can be recorded in the ticket cache (Kerberos 1.11)
- Monitoring of the ticket expiration
  - Core functionality is built
  - Needs to be integrated into OS as a service that can be interacted with over D-BUS
  - Desktop ticket renewal dialog needs to become a subscriber

GSS Proxy

- Goal: make dealing with Kerberos tickets in the GSSAPI context simple and overcome existing limitations
- Was discussed a year ago at the conference
- Project started right after

GSS Proxy



If a service is compromised, keytab is not compromised and still can be trusted to do PAC validation.

GSS Proxy

- Privilege separation (client and server)
  - Service that talk over the network do not have access to keytab
- Kerberos ticket size restriction (server)
  - Linux Kernel has some limitations
- MS-PAC extraction (client in case of trust)
  - GSS Proxy does it instead of the service itself
- Ticket renewal (client)
  - Tickets are automatically re-acquired – no need for k5start

GSS Proxy Next Steps

- Make it more stable and better configurable via INI file
- Kernel patches need to be committed for the server side integration
- GSSD needs to be updated to take advantage of GSS Proxy
- SSSD need to take advantage of the GSS Proxy
- GSS Proxy needs to be able to renew special service tickets using application accounts with keytabs

Key Rotation

- Intent:
  - Create a service that would be able periodically based on the policy fetch a new keytab instead of the existing one
- Project was taken and delivered as a Master thesis
  - Will be integrated with SSSD to rotate keytabs against AD and FreeIPA
  - Planned for SSSD 1.10 and Fedora 19 (spring 2013)

Ticket Cache Type and Location

- Kerberos 1.10 delivered couple features:
  - DIR style ticket cache
  - Ability to choose which ticket to use based on the identity if the service principal
- In Fedora 18 all Kerberos enabled applications:
  - switched to using ticket cache from common location (/run/user instead of /tmp)
  - ticket type by default is DIR instead of FILE

End-to-end SC support

- System Security Services Daemon (SSSD) improvements:
  - Add SC support
  - Add PKINIT support
- FreeIPA improvements:
  - Add automatic support for PKINIT

Authorization

- PAD specification needs to be taken to IETF
- We need to understand what that means to support similar claims functionality as the one delivered by Microsoft in Windows Server 2012
    - Need to go through standardization
- Levels of assurance as part of the Kerberos authorization data is still an open question

Summary

Red Hat will continue working with MIT Kerberos consortium and MIT Kerberos developer community to build Kerberos features needed to make the projects outlined in this presentation successful and deliver value to customers and communities.

Questions?