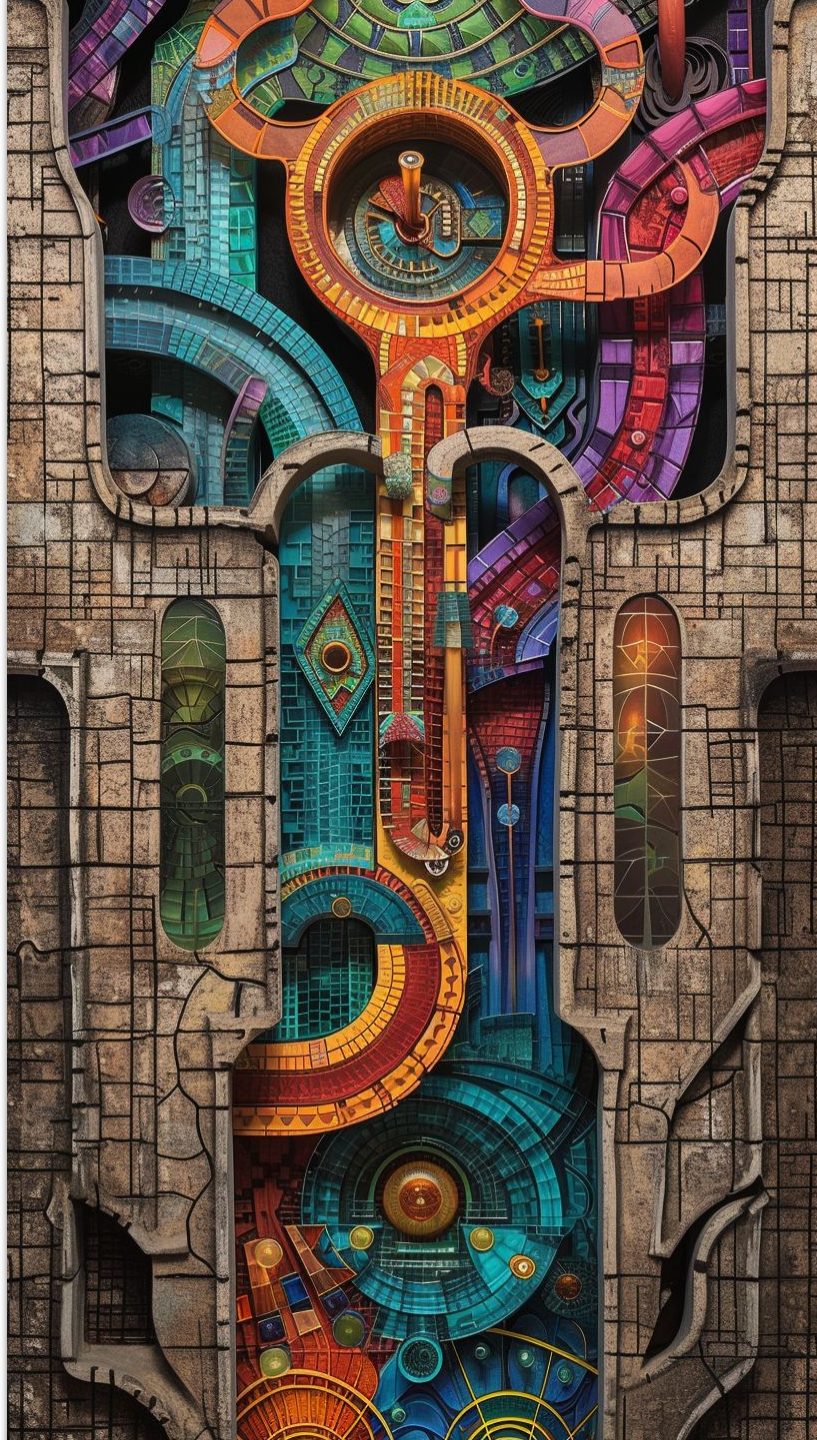
sambaXP'2024

Get rid of NTLM or become passwordless: choose both?

Alexander Bokovoy || Andreas Schneider



Who are we?

Alexander Bokovoy

- Software Engineer at Red Hat
- Focus on identity management and authentication in Red Hat Enterprise Linux and Fedora Project
  - FreeIPA, SSSD, Samba, MIT Kerberos
- Samba Team member, FreeIPA core developer

Andreas Schneider

- Software Engineer at Red Hat
- Samba maintainer for Red Hat Enterprise Linux and Fedora Project
- FOSS Hacker: Samba, MIT Kerberos, libssh, cmocka, cwrap, neovim ...
- Samba Team member

The evolution of Windows authentication

- Microsoft, October 2023:
  - https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848

> Our end goal is eliminating the need to use NTLM at all to help improve the security bar of authentication for all Windows users.

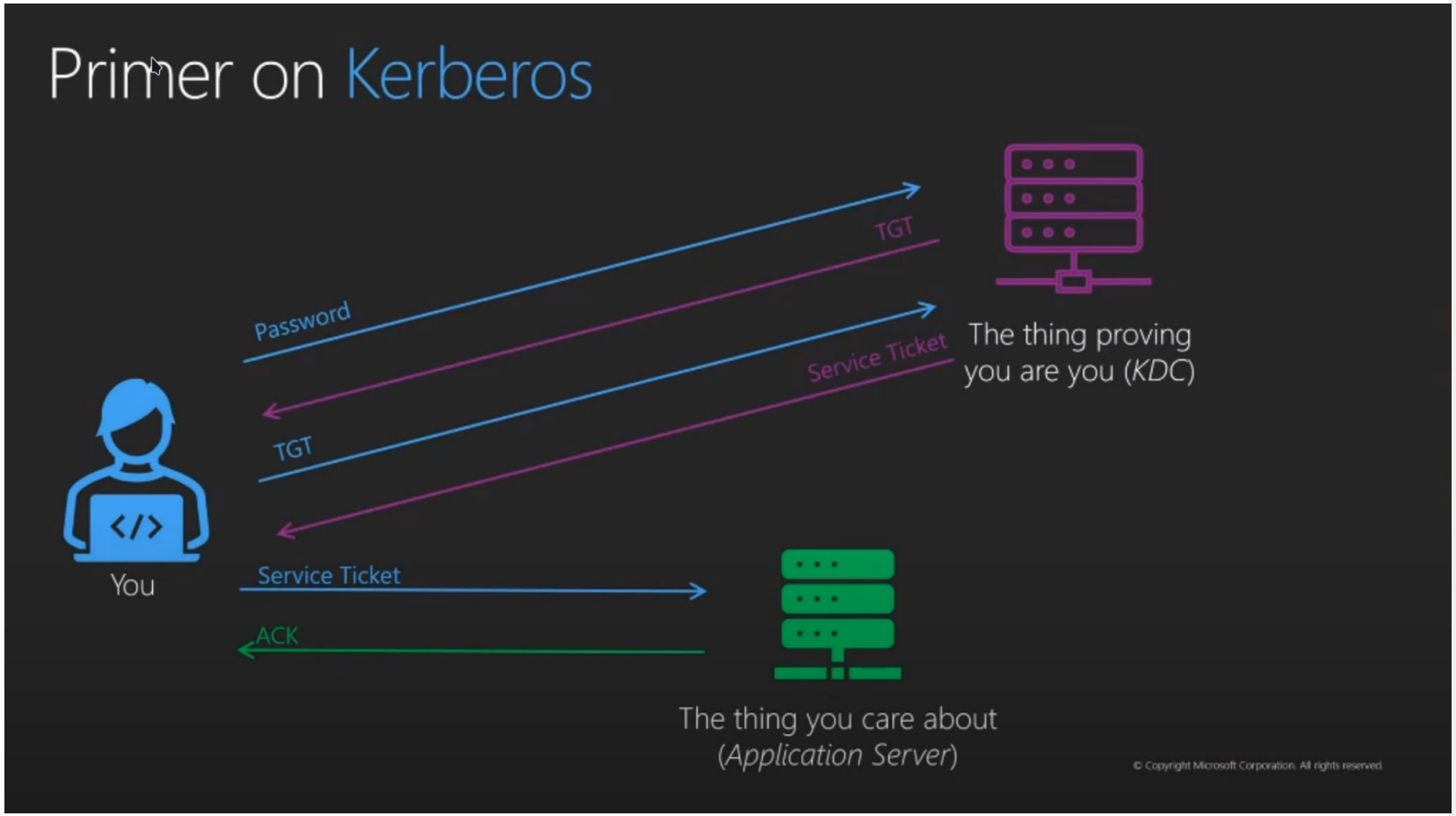
Kerberos, better than ever

For Windows 11, we are introducing two major features to Kerberos to expand when it can be used—addressing two of the biggest reasons why Kerberos falls back to NTLM today. The first, IAKerb, allows clients to authenticate with Kerberos in more diverse network topologies. The second, a local KDC for Kerberos, adds Kerberos support to local accounts.

- Microsoft, March 2024: "The Evolution of Windows Authentication" presentation

The evolution of Windows authentication

- Kerberos



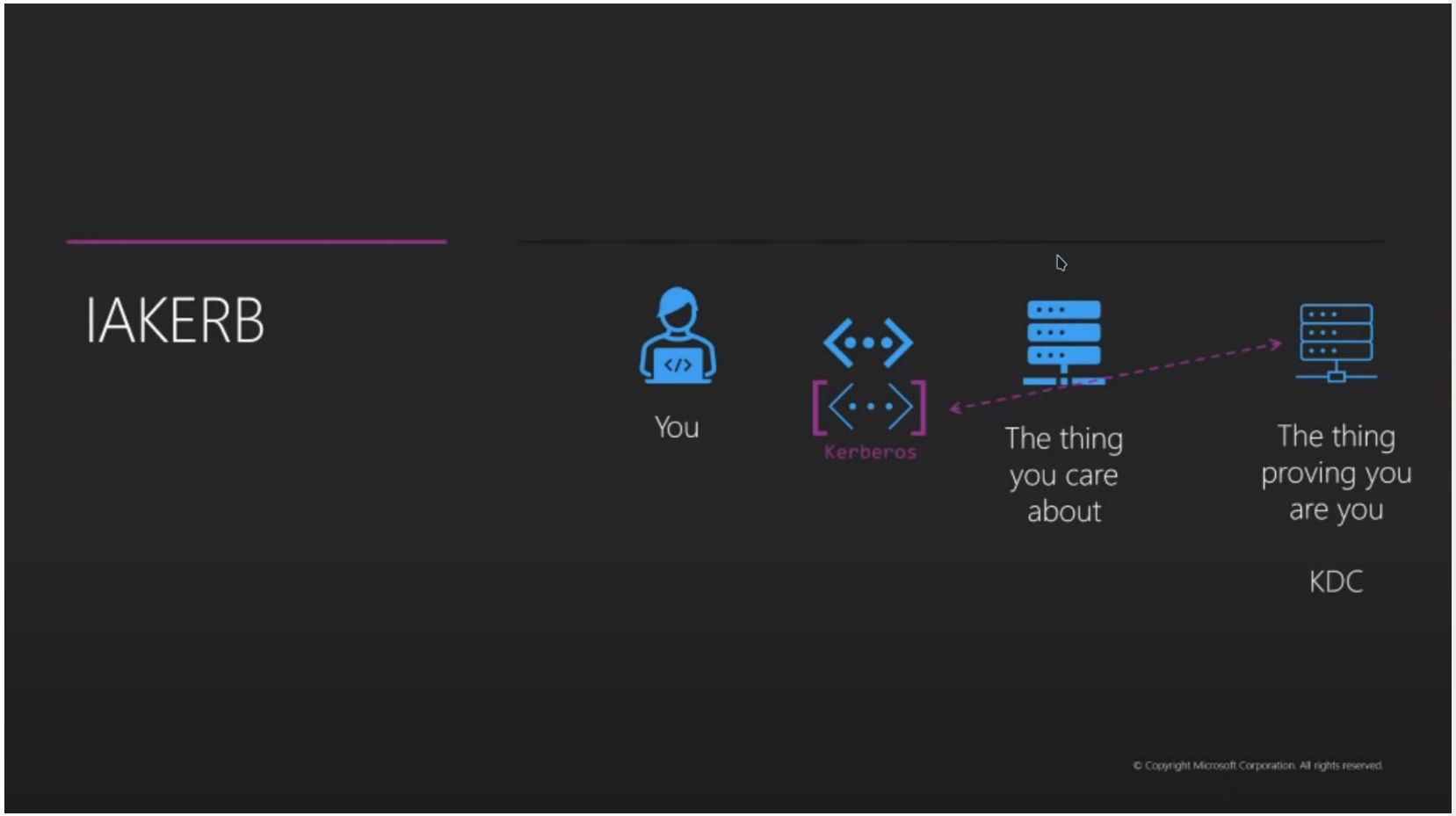
sssd
SAMBA TEAM
FreeIPA
Open Source Identity Management Solution

The evolution of Windows authentication

- Line of Sight

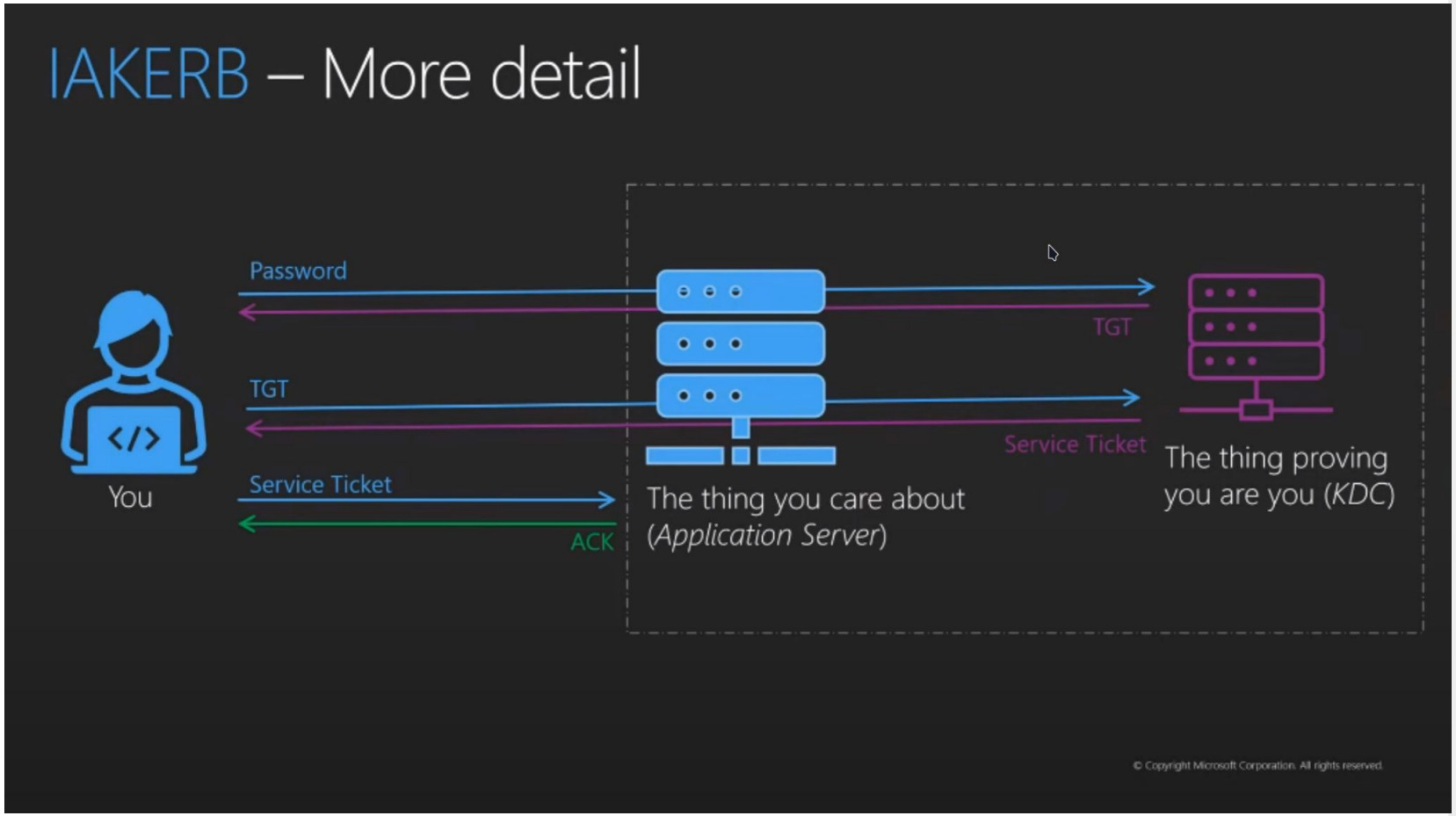
The evolution of Windows authentication

- Kerberos + IAKerb (Initial and pass through authentication using SPNEGO)



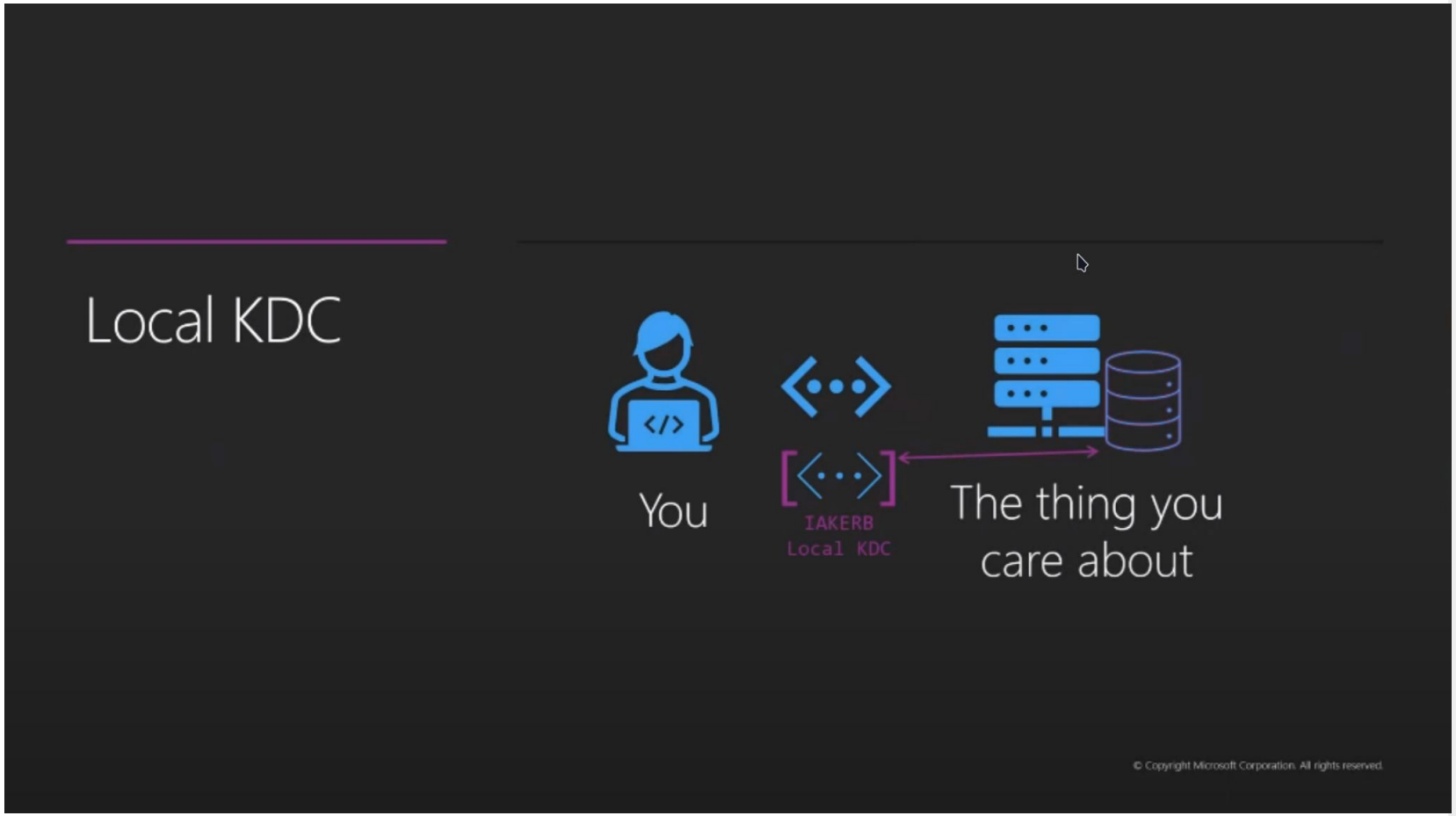
The evolution of Windows authentication

- Kerberos + IAKerb (Initial and pass through authentication using SPNEGO)



The evolution of Windows authentication

- IAKerb + LocalKDC



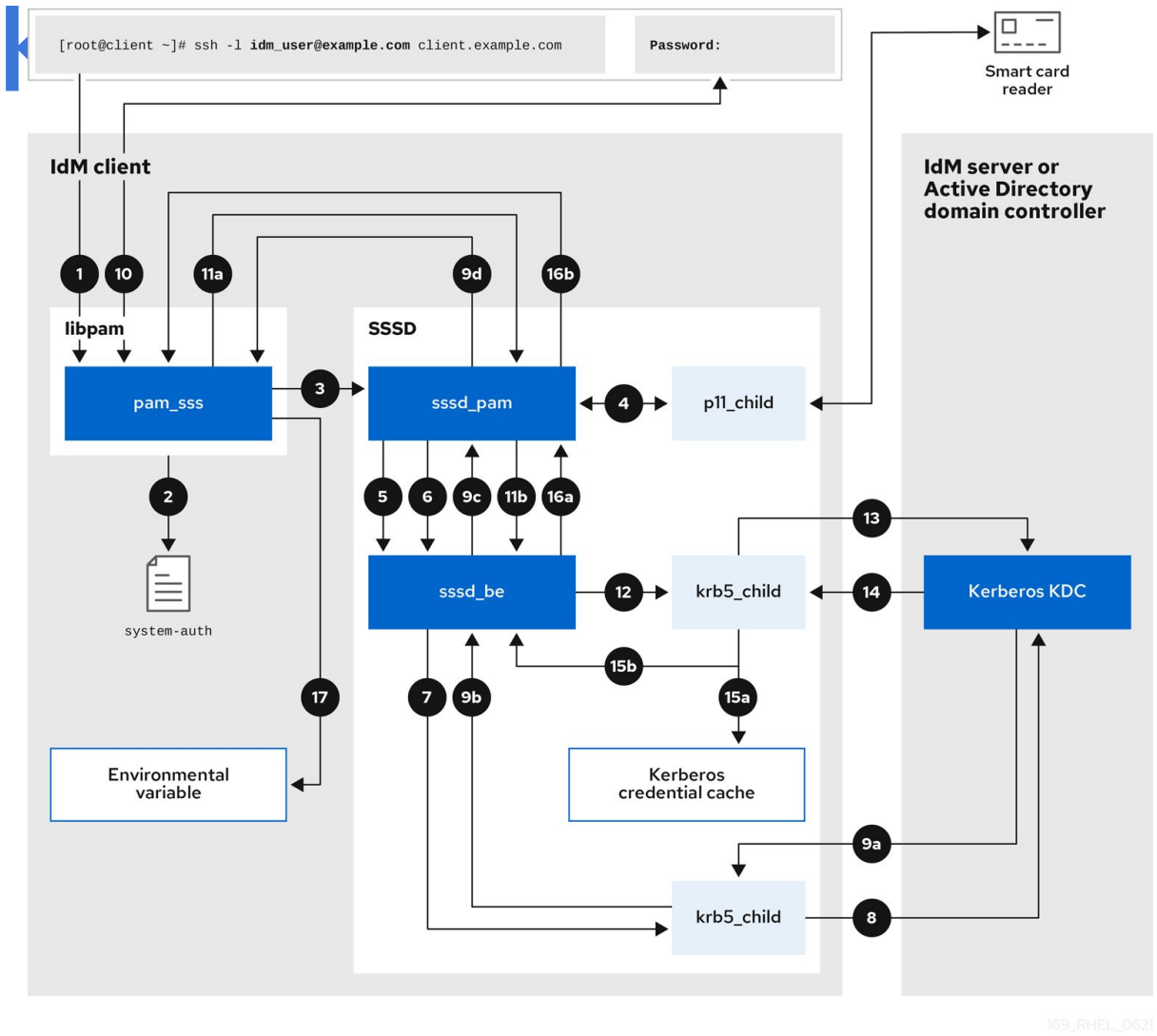
Similar needs

- Support OAuth2 authorization and authentication, support for passwordless methods
  - Done with RHEL IdM (FreeIPA) and Kerberos, demand for non-IdM environments as well
- Support environments with heavy firewalls (lack of direct line of sight)
  - Kerberos KDC proxy
    - Integrated in FreeIPA
    - Supported by MIT Kerberos and Windows clients
- FIPS environments
  - Strict cryptography requirements, no NTLM or RC4 anymore
- Kerberos is a natural choice (with RFC 8009 encryption types)

Passwordless authentication

- FreeIPA + SSSD
  - ipa-otpd ‘RADIUS’ backend to MIT Kerberos KDC, originally to enable RADIUS pass-through and TOTP/HOTP authentication in FreeIPA
  - Kerberos pre-authentication methods by SSSD for external OAuth2 authorization and FIDO2 authentication for MIT Kerberos
- Demo at SambaXP’23, slides

Authentication with



Detailed description is in RHEL IdM guide 'Configuring and managing Identity Management': 8.3. Data flow when authenticating as a user with SSSD in IdM

Kerberos

- User identities are decoupled from the authentication identities
  - POSIX environment needs user/group identities
  - Kerberos KDC does not need POSIX identities
  - FreeIPA and Samba AD tie POSIX and Kerberos identities via PAC information in the Kerberos tickets
    - * MIT Kerberos 1.20+ also issues mini-PAC

Local Kerberos KDC

- What if:
  - Reuse FreeIPA/SSSD experience and modules, use default MIT Kerberos backend and configuration as much as possible in a standalone setup?
- MIT Kerberos KDC is lightweight and easy to set up
- [Prototype]
  - https://github.com/abbra/local-kdc

Local Kerberos KDC

- Configuration:
  - KDC listens on localhost (127.* (better would be a unix socket))
  - Use HOSTNAME as a Kerberos realm
  - Users can be defined elsewhere in the system
  - Kerberos principals match usernames and KDC database only contains information about the Kerberos keys
  - SSSD is used to bridge Kerberos authentication and users

Local Kerberos KDC

- Usage:
  - Password-based login
    - SSSD will handle acquisition of the Kerberos ticket locally
  - Kerberos-based login
    - If you have access to the KDC, you can acquire the ticket and use it against all local services that support GSSAPI
      - Cockpit, CUPS, etc.

- pam_sss handles authentication
  - Can handle Kerberos pre-authentication methods' prompts

- pam_sss_gss handles Kerberos ticket authentication
  - Allows to authenticate with existing Kerberos ticket for any PAM application

Local Kerberos KDC

- What pre-authentication methods are supported out of the box?
  - Password-based:
    - timestamp and SPAKE
  - Keytab-based:
    - timestamp and SPAKE
  - Smart Cards or certificates:
    - PKINIT

- Works with Samba in a file server only mode (standalone) (work in progress for Samba 4.21)
  - [prototype]

Samba and local KDC

- File server only (standalone) mode
  - passdb backend handles user information required by SMB
  - System-wide NSS handles POSIX information
  - Allows Kerberos tickets to be used if Kerberos principal is mapped to the POSIX user

- Samba did not expect a PAC in file server only mode
  - PAC contains multiple buffers, including logon information
  - This is the only mode working with pure Kerberos realms
  - MIT Kerberos 1.20+ added mini-PAC to mitigate Kerberos protocol attacks
    - mini-PAC has several checksums and a logon name
  - Fixed in Samba git master

Samba and local KDC

- Samba did not expect RFC 8009 encryption types
  - RFC 8009 defines AES variants with SHA-2 HMAC
  - FIPS 140-3 compliant
    - Not supported by Windows yet (planned for Windows Server 2025?)
  - MIT Kerberos defaults to RFC 8009 on Fedora and RHEL unless overridden by the local configuration (Samba AD DC/MIT)
  - Fixed for Samba 4.21 and backported to 4.20.x release (bug 15635)

Local Kerberos KDC

- What about passwordless methods from FreeIPA?
  - Can we add them?
- Sure!
  - MIT Kerberos KDC supports a RADIUS-based backend channel
    - UNIX domain socket to talk to if KDC driver hints to a pre-authentication method that a principal has been enabled for this method
      - Used by ‘otp’, ‘idp’, and ‘passkey’ methods
    - KDC side of a pre-authentication method uses RADIUS packet over UNIX domain socket to query for authorization details
    - Returned information from a RADIUS ‘server’ is then conveyed to the client side of the pre-authentication method
    - Requires FAST channel presence

Local Kerberos KDC

- What about passwordless methods from FreeIPA?
  - Can we add them?
- Sure!
  - FreeIPA provides `ipa-otpd` daemon as the RADIUS backend
    - Pulls Kerberos principal authentication method details from LDAP
    - Uses LDAP bind for TOTP/HOTP verification
    - Can forward request to a real RADIUS server
    - Calls out for oidc_child from SSSD for OAuth2
    - Calls out for passkey_child from SSSD for FIDO2
- We don't have LDAP server locally
  - Refactor `ipa-otpd`
    - Allow using local configuration instead
    - Work in progress

Local KDC: IAKerb

- IAKerb is part of GSSAPI specifications
  - Implemented in MIT Kerberos
    - Draft version, needs a refresh to work against new Windows
  - Not implemented in Heimdal
    - There is IAKerb implementation in the Apple's fork

- Triggered by use of IAKerb mech in GSSAPI negotiation
  - Example: MIT's gss-sample demo app uses -iakerb option to replace mech OID when client talks to the server (and server accepts it)
  - Samba hardcodes use of krb5 mech OID

Local KDC: IAKerb

- Passwordless pre-auth methods
  - Require prompt exchanges
    - `passkey`:
      - Insert your passkey device, then press ENTER:
      - Enter PIN:
      - Please touch your device
    - `idp`:
      - Authenticate at https://some.site/auth/device?user_code=YHMQ-XKTL and press ENTER.:
- Prompting is not supported in GSSAPI
  - GSSAPI context may be exported and imported across processes, need an API to explicitly handle prompts
    - Some context is in https://github.com/krb5/krb5/pull/1335

Local KDC: IAKerb alternative

- Kerberos KDC proxy protocol [MS-KKDCP]
  - HTTPS end-point to access remote KDC
  - https://github.com/latchset/kdcproxy/
  - Supported by MIT Kerberos clients
  - Not supported by Heimdal
    - Broken support by Apple's Heimdal fork
  - Works with raw Kerberos, works with passwordless methods
    - But adding refreshed IAKerb and prompting would be great

MIT Kerberos (ToDo)

- Update IAKerb implementation (only draft implemented)
- Add GSSAPI support for prompters
- Nice to have:
  - Support for unix domain sockets
  - Support for socket activation
  - KDB module for basic local KDC support

Samba ToDo

- To-Do: Kerberos instead of NTLM
  - Our SPNEGO implementation needs to recognize IAKerb
  - Domain member <> domain controller communication
    - Netlogon schannel setup: NetrServerAuthenticate3 -> NetrServerAuthenticateKerberos
    - PAC validation and ticket forwarding netlogon calls
  - The client command line tools need to be adapted for IAKerb
  - KDB module for local KDC with passdb support to provide logon information
  - Add member support for multiple domains

Thank you!


sssd
SAMBA
TEAM
FreeIPA
Open Source Identity Management Solution