Enabling FIDO2/WebAuthn support for remotely managed users

FOSDEM 2023

Iker Pedrosa
Software Engineer

Alexander Bokovoy
Sr. Principal Software Engineer

Red Hat

Agenda

- Introduction
- Reality
- High level overview
- Testing playground
- Feedback and questions

Introduction

Why FIDO2/WebAuthn?

- Passwordless
- Enables strong authentication
- Reduces the risk of a data breach
- Reduces phishing threads

FIDO2/WebAuthn workflows

- User authentication in a website
- Local user authentication in a Linux system
- Passwordless authentication in Windows

Objective

- **FIDO2/WebAuthn** authentication
- Remotely managed users
- Local authentication
- Remote authentication

Reality

US government memo

- Zero Trust Model
- Centralized identity management systems
- Phishing-resistant MFA
- Sign in once

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks. The Federal Government's Personal Identity Verification (PIV) standard is one such approach. The World Wide Web Consortium (W3C)'s open "Web Authentication" standard,[8] another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services.

Agencies must require their users[9] to use a phishing-resistant method to access agency-hosted accounts. For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications.

This requirement for phishing-resistant methods is necessitated by the reality that enterprise users are among the most valuable targets for phishing. That problem can be mitigated by providing those users with phishing-resistant tokens, including the PIV cards that agency staff and partners are generally issued.

FIDO2 workflow for remotely managed users

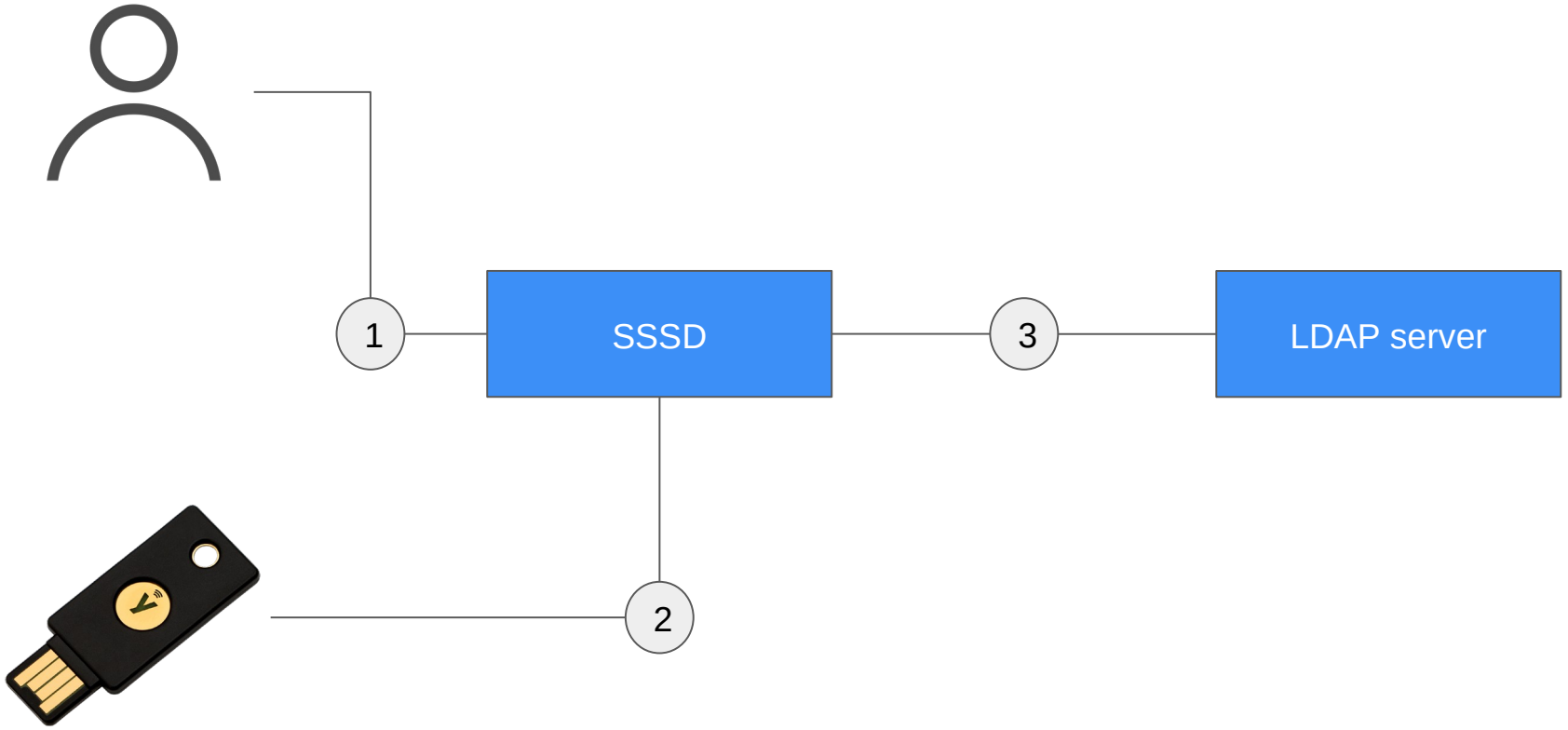
- Key registration
- Store public key in LDAP attribute
- Local authentication with FIDO2 key
- Kerberos ticket issuance

High level overview

Technologies involved

- FIDO2/WebAuthn
- LDAP server
- Kerberos
- SSSD

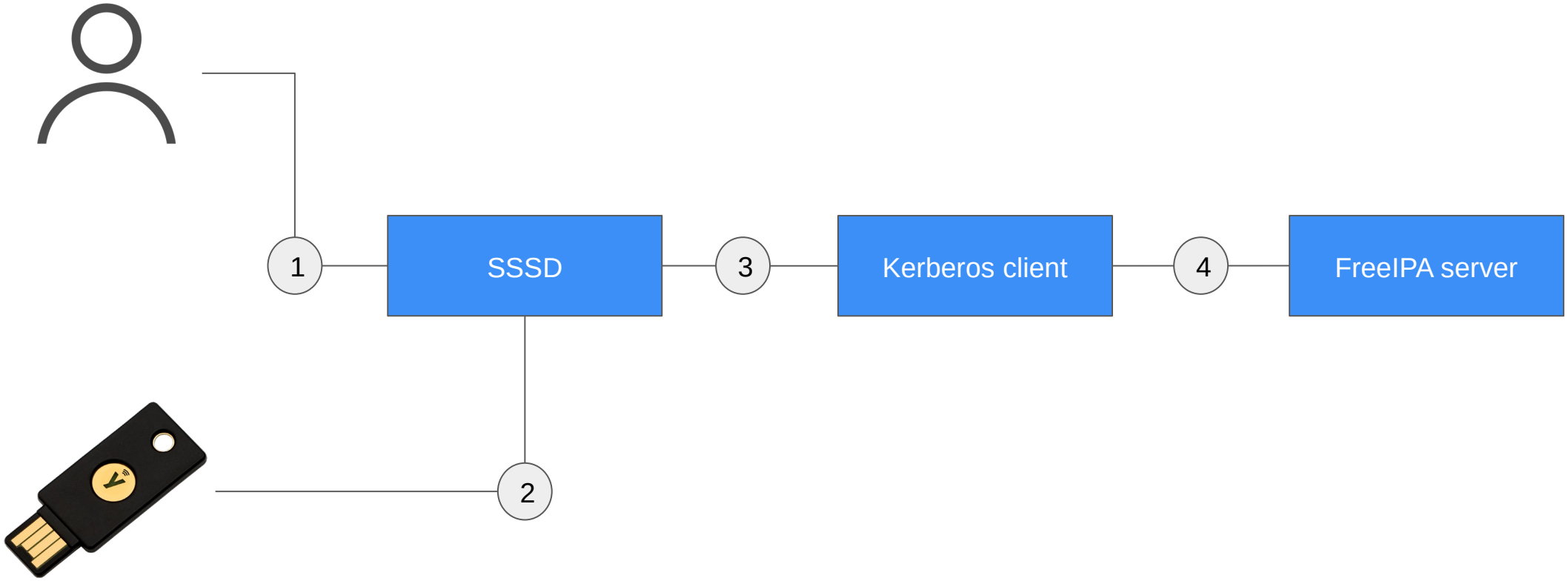
Local authentication



```
# abokovoy, users, accounts, some.domain
dn: uid=abokovoy,cn=users,cn=accounts,dc=some,dc=domain
objectclass: ipaobject
objectclass: person
objectclass: top
objectclass: ipasshuser
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: krbticketpolicyaux
objectclass: krbprincipalaux
objectclass: inetuser
objectclass: posixaccount
objectclass: ipaSshGroupOfPubKeys
objectclass: mepOriginEntry
objectclass: ipauserauthtypeclass
objectclass: ipantuserattrs
objectclass: ipapasskeyuser
[.... ....]
ipapasskey: passkey:[.... .....]
ipapasskey: passkey:[.... .....]
```

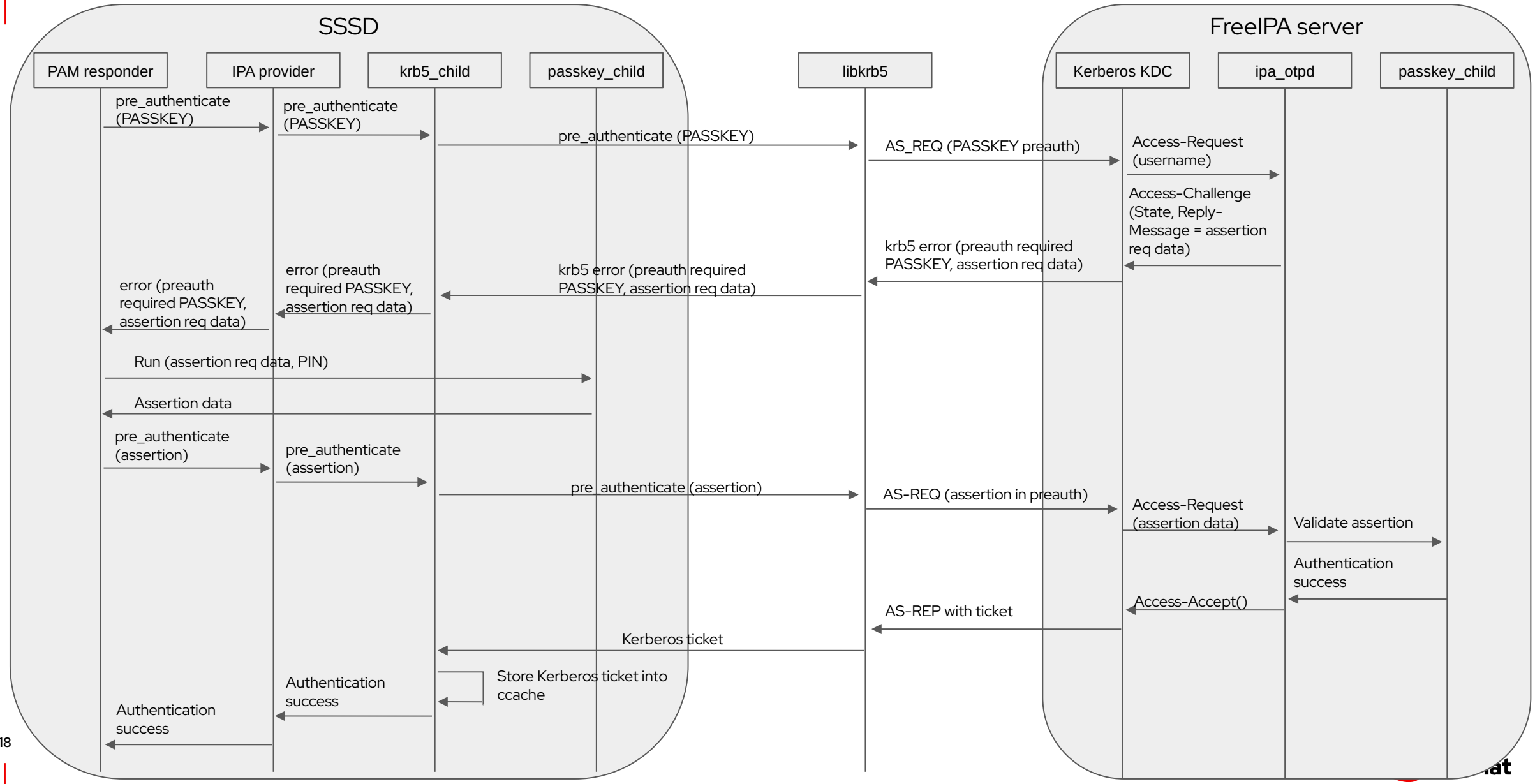
```
$ ipa user-show abokovoy
  User login: abokovoy
  First name: Alexander
  Last name: Bokovoy
  Home directory: /home/abokovoy
  Login shell: /bin/bash
  Principal name: abokovoy@SOME.REALM
  Principal alias: abokovoy@SOME.REALM
  Email address: ab@some.email
  UID: 1000
  GID: 1000
  Telephone Number: [... ...]
  User authentication types: password, otp
  Certificate: [... ....]
  Passkey mapping: passkey:[.... ....]
                   passkey:[.... ....]
  Account disabled: False
  Password: True
  Member of groups: gitrepo, system-admins, smime_users, ipausers, audio, usb-access, admins
  Roles: Certificate Auditor
  Subordinate ids: ad0dad02-99bf-43ef-8594-d8cd20be882b
  Indirect Member of group: admin, ca-kerberos-services-acl-users, wheel
  Indirect Member of Sudo rule: admins
  Kerberos keys available: True
```

Kerberos integration (FreeIPA only)

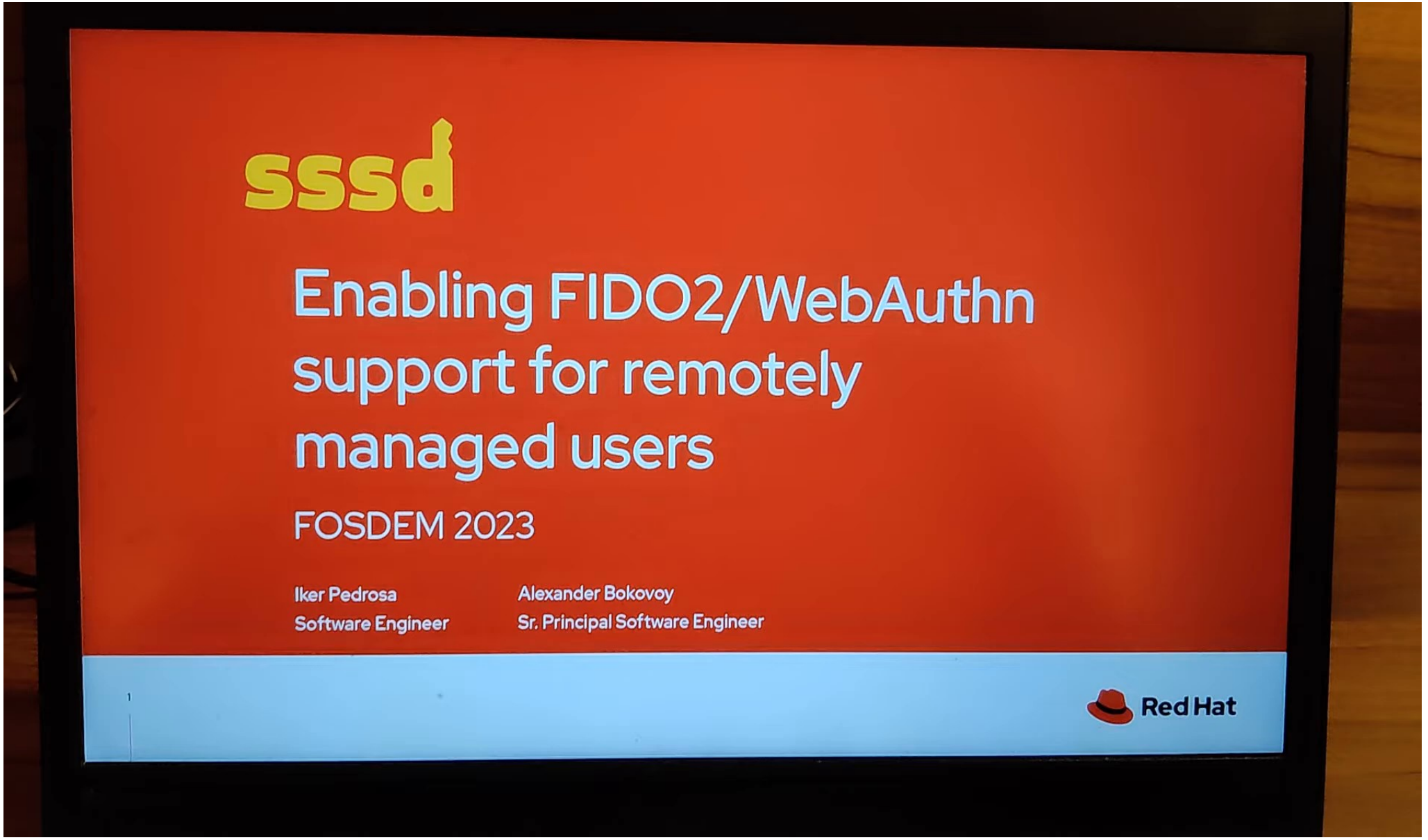


Red Hat

High level overview



Testing playground


sssd
Enabling FIDO2/WebAuthn support for remotely managed users
FOSDEM 2023
Iker Pedrosa
Software Engineer
Alexander Bokovoy
Sr. Principal Software Engineer
1
Red Hat

Instructions

- https://ikerexxe.github.io/idm/2022/12/19/passkey-central-auth.html

Fedora 36/37:
Test COPR repository: ipedrosa/passkey-auth

```
dnf copr enable ipedrosa/passkey-auth
dnf update sssd-*
dnf install sssd-passkey

/etc/sssd/conf.d/passkey-enable.conf (root, root, 0600)
----------------------------------------------
[pam]
pam_passkey_auth=true
```

Feedback and questions

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat