Passwordless Linux

Passkey and External IdP login with FreeIPA

Fraser Tweedale

@hackuador[@functional.cafe]

About me

- 10 years at Red Hat working on **PKI** and **identity management**
- >15 years working software engineer
- Love functional programming and especially Haskell

Acknowledgements

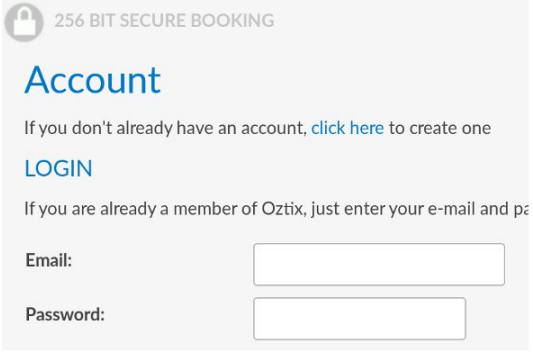
- I didn't work on any of the cool stuff I'm demoing today
- **Alexander Bokovoy**, **Iker Pedrosa**, and **many others** (FreeIPA / SSSD)
- **Ray Strode** (GNOME)

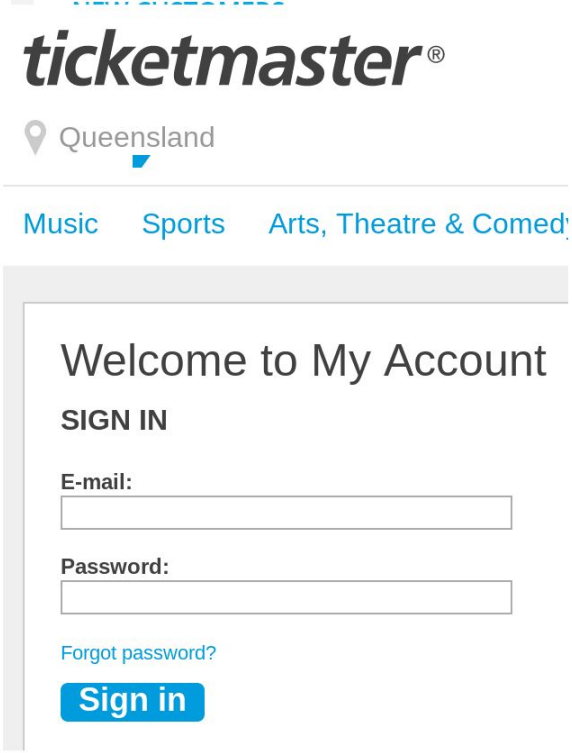
Outline

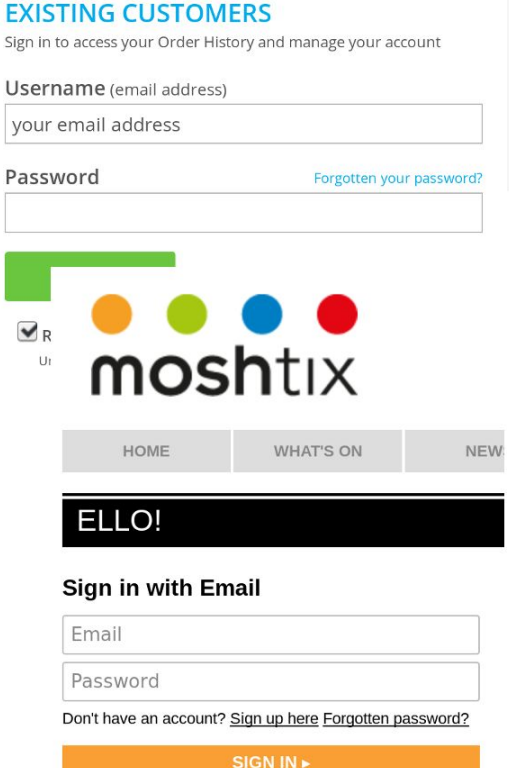
- **Why** NOT passwords
- Alternatives to passwords
- FreeIPA overview
- **Demo**
- Boring technical stuff
- Resources

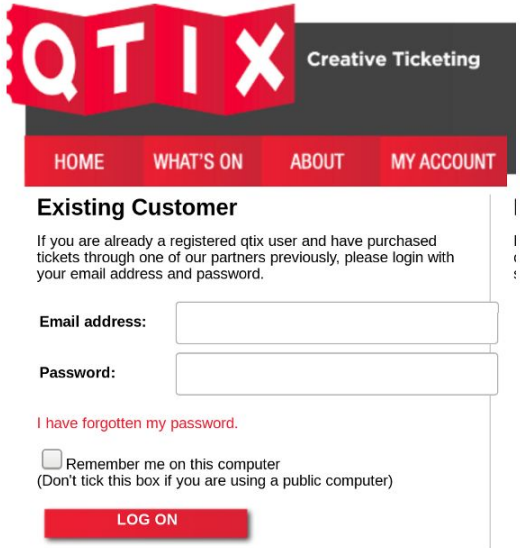

TICKETEK


oztix
HOME
EVENT GUID


256 BIT SECURE BOOKING
Account
If you don't already have an account, click here to create one
LOGIN
If you are already a member of Oztix, just enter your e-mail and pa
Email:
Password:


ticketmaster®
Queensland
Music
Sports
Arts, Theatre & Comed
Welcome to My Account
SIGN IN
E-mail:
Password:
Forgot password?
Sign in


EXISTING CUSTOMERS
Sign in to access your Order History and manage your account
Username (email address)
your email address
Password
Forgotten your password?
moshtix
HOME
WHAT'S ON
ELLO!
Sign in with Email
Email
Password
Don't have an account? Sign up here Forgotten password?
SIGN IN


QTIX
Creative Ticketing
HOME
WHAT'S ON
ABOUT
MY ACCOUNT
Existing Customer
If you are already a registered qtix user and have purchased tickets through one of our partners previously, please login with your email address and password.
Email address:
Password:
I have forgotten my password.
Remember me on this computer
(Don't tick this box if you are using a public computer)
LOG ON

Hackers nab 1.2B passwords in colossal breach, says security firm

Dropbox Forces Password Resets After User Credentials Exposed

Change your password! Yahoo confirms data breach of 500 million accounts

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

43 million passwords hacked in Last.fm breach

Passwords

- We're all tired of passwords, aren't we?
- Many users are **not diligent** (weak; reuse)
- Many users are not **technically proficient** (what's a password manager?)
- Using passwords securely imposes **friction** and **cognitive load**
- Complexity and rotation policies **DO NOT HELP!**
- **Phishing risk**, even for technical users

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.

M-22-09 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

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.

M-22-09 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Objectives

- Reduce **password risks** (weak, reused, …)
- Reduce **phishing** risks
- Reduce **friction** for users (make it quick and easy)
- Reduce **frequency** of explicit user authentication (single sign-on)
- Through a combination of the above, **improve security** posture

Alternatives to (only) passwords

- Two-factor authentication
- Smartcards
- Passkeys / WebAuthn
- Web SSO providers

Two-factor authentication

- a.k.a. **2FA**, multi-factor authentication (**MFA**)
- Password **plus** a one-time code
- HOTP / TOTP / SMS / hardware token
- **Phishable**

Smart cards

- Cryptographic token with (optional) PIN
- Private key + **X.509 certificate**
- Sign a challenge to prove identity
- **Phishing-resistant**
- Issuance, **renewal** and **revocation** complexities
- USB, NFC, "SIM-esque", …

Everything Open 2024

Passkeys / WebAuthn

- Cryptographic token with (optional) PIN
- Optional physical presence check (touch the token)
- Optional **token attestation**
- Unique private keys bound to websites (or other RPs)
- Sign a challenge to prove identity
- **Phishing-resistant**
- *"Passkey"* ≅ FIDO2 ≅ W3C WebAuthn + CTAP

W3C®

Everything Open 2024

fido™ ALLIANCE

Web SSO

- SAML / **OAuth 2.0** / **OpenID Connect**
- Use an existing account to authenticate
- For public sites: offered by many popular public services (**privacy concern**)
- For organisations: Keycloak, Red Hat SSO, many SaaS offerings
- Works great for web; *can* work for other scenarios

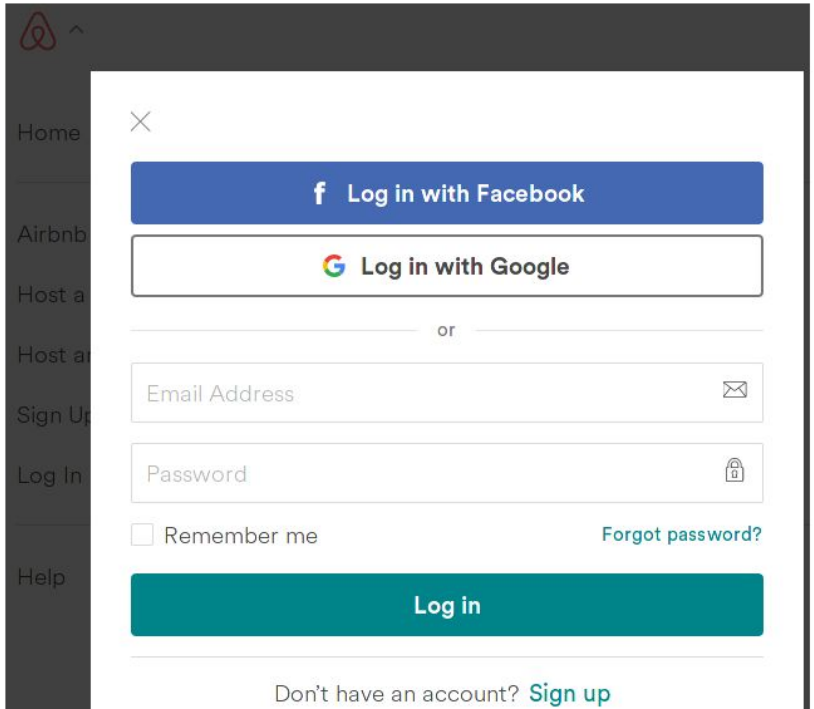
Travis CI Blog Status Help

Sign in with GitHub

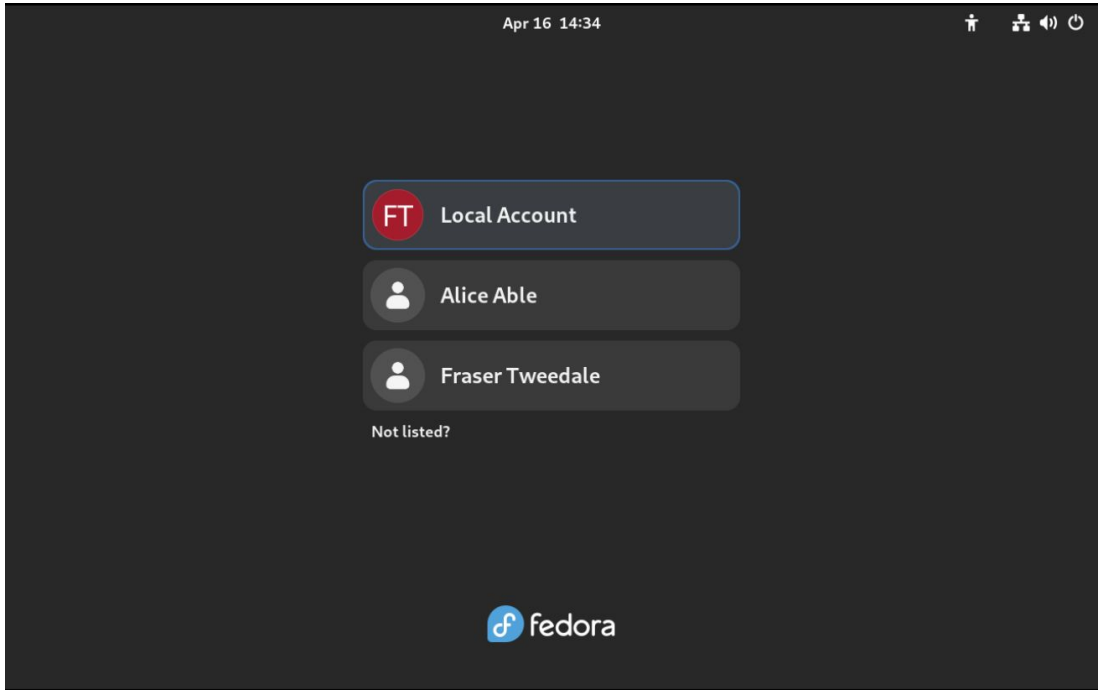
Test and Deploy with Confidence

Easily sync your GitHub projects with Travis CI and you'll be testing your code in minutes!

Sign Up



Workstation login



Everything Open 2024

Workstation login - **standalone**

- Password ✅ `pam_unix`
- 2FA ✅ `pam_2fa, pam_oath, pam_yubico, ...`
- Smartcard ✅ `pam_pkcs11`
- Passkey ✅ `pam_u2f`
- Web SSO ❓

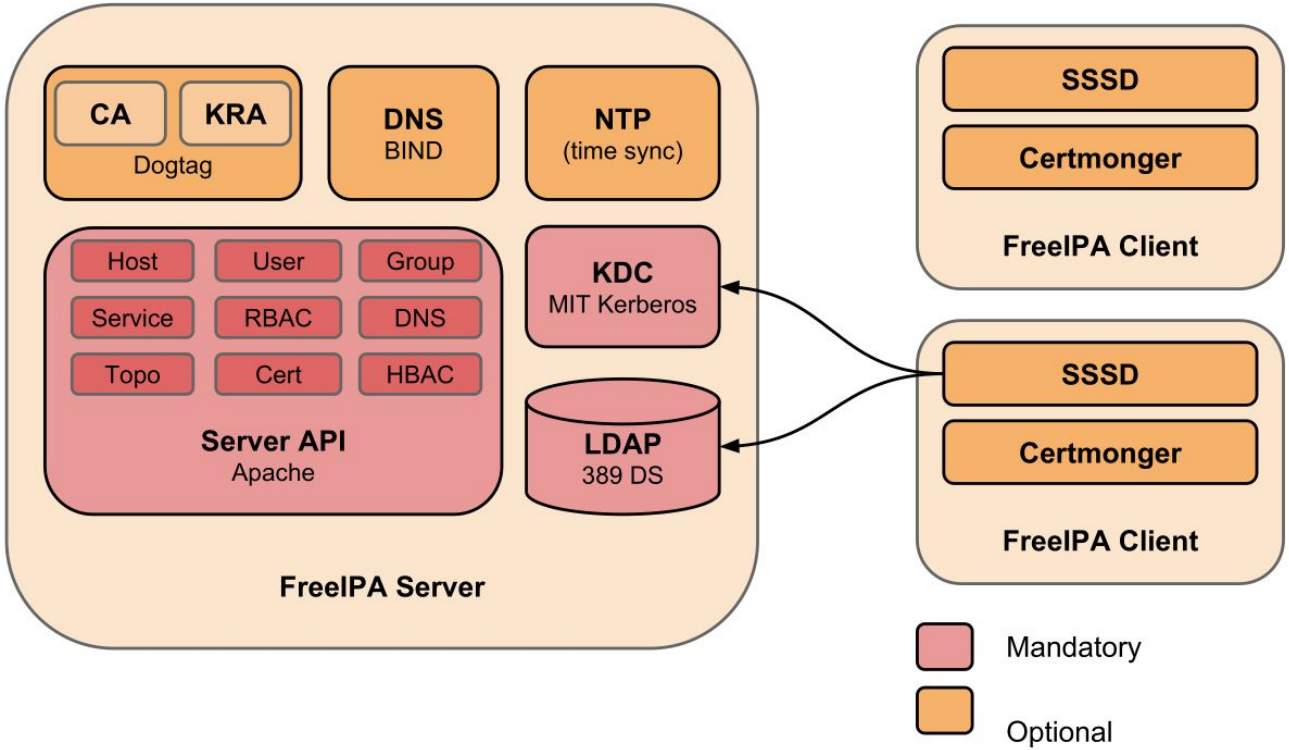
Workstation login - **domain member**

- Password ✅ `pam_sss`
- 2FA ✅ `pam_sss`
- Smartcard ✅ `pam_sss`
- Passkey ✅ `pam_sss`
- Web SSO ✅ `pam_sss`

FreeIPA / Red Hat Identity Management

- Centralised identity management for Linux/UNIX environments
- **Authentication**: Kerberos, password, 2FA, Smartcard, Passkey, OIDC IdPs
- **Policy**: HBAC, Sudo rules, SELinux maps, PKI, …
- Cross-realm trusts with Active Directory
- Fedora + RHEL (server) ; most distros (client)
- Public demo instance: https://www.freeipa.org/page/Demo
- Ansible roles: https://github.com/freeipa/ansible-freeipa

FreeIPA - architecture



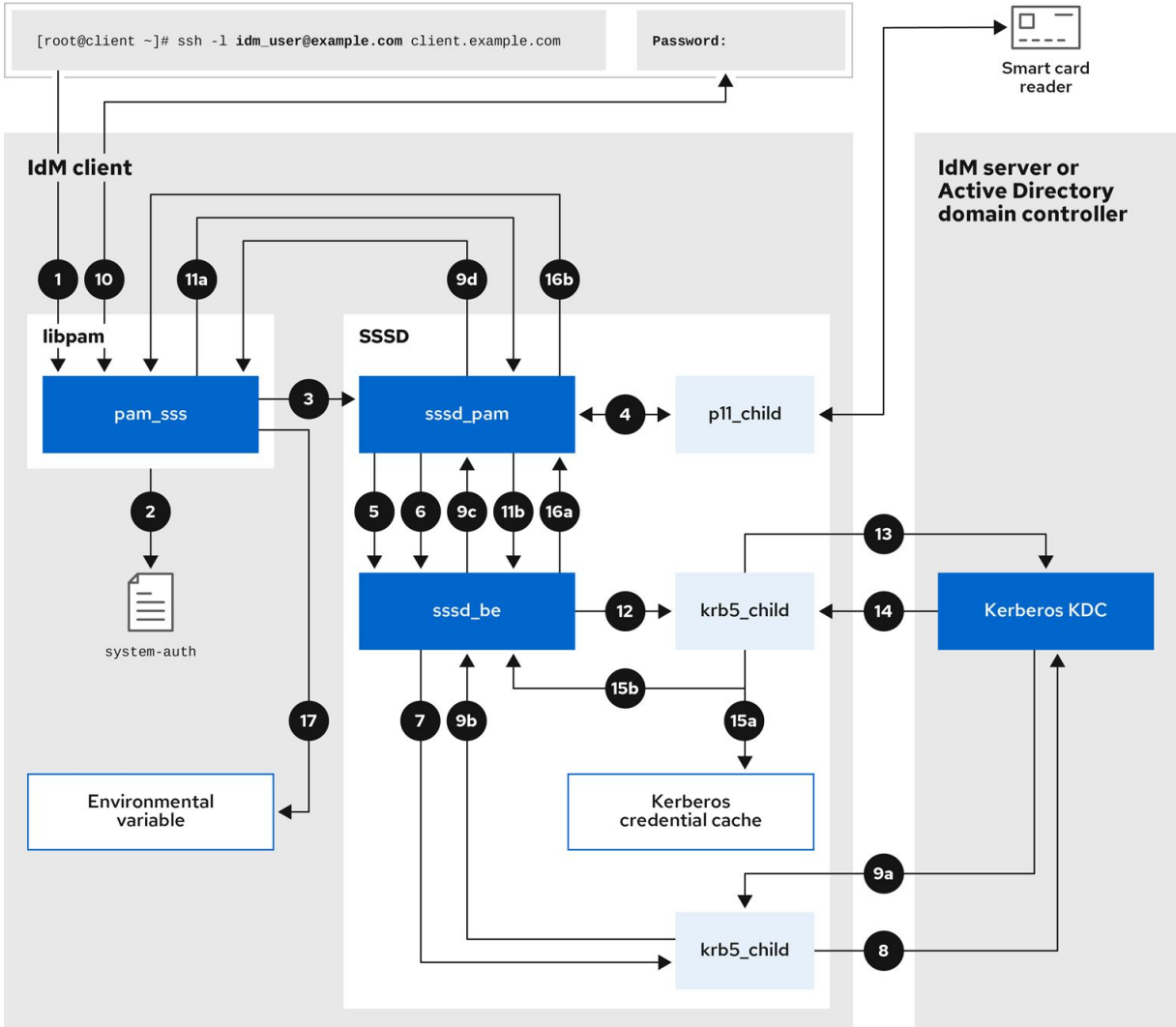
Demo

How does this even work?

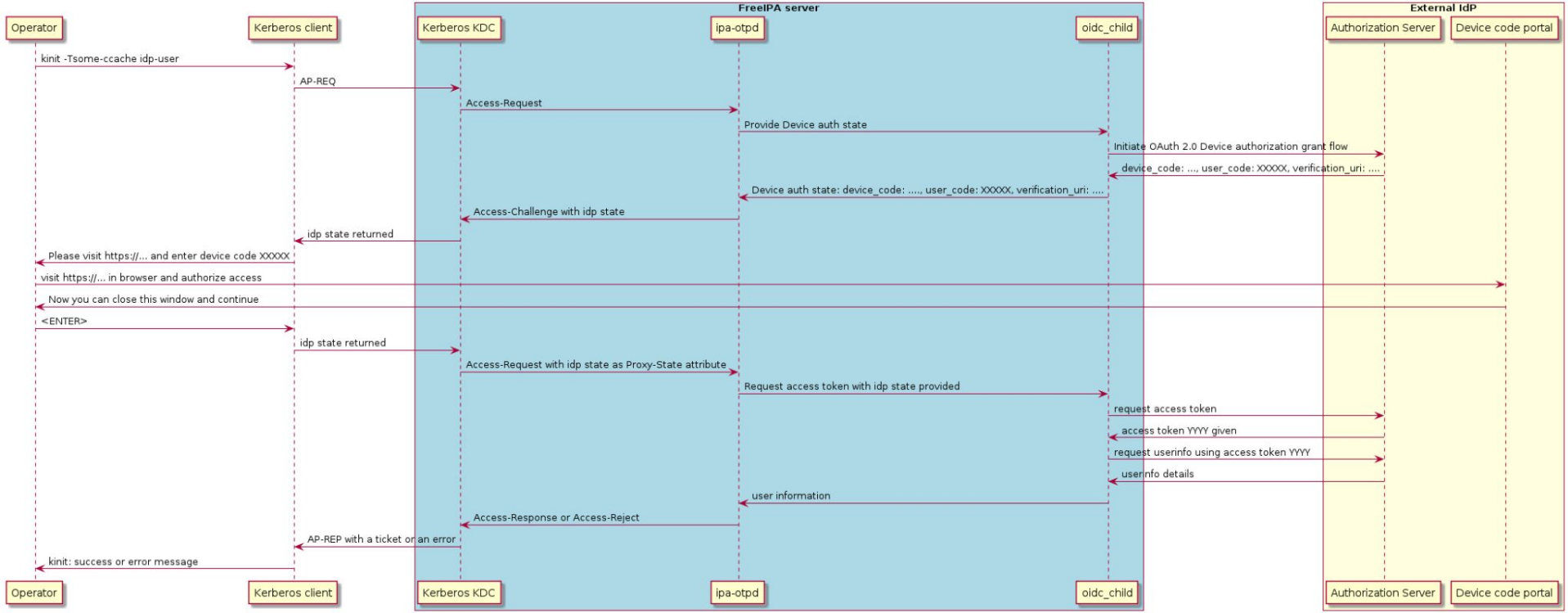

Always has been
Wait, it's all Kerberos?

Smart card

Diagram from RHEL guide *'Configuring and managing Identity Management'*: [8.3. Data flow when authenticating as a user with SSSD in IdM]

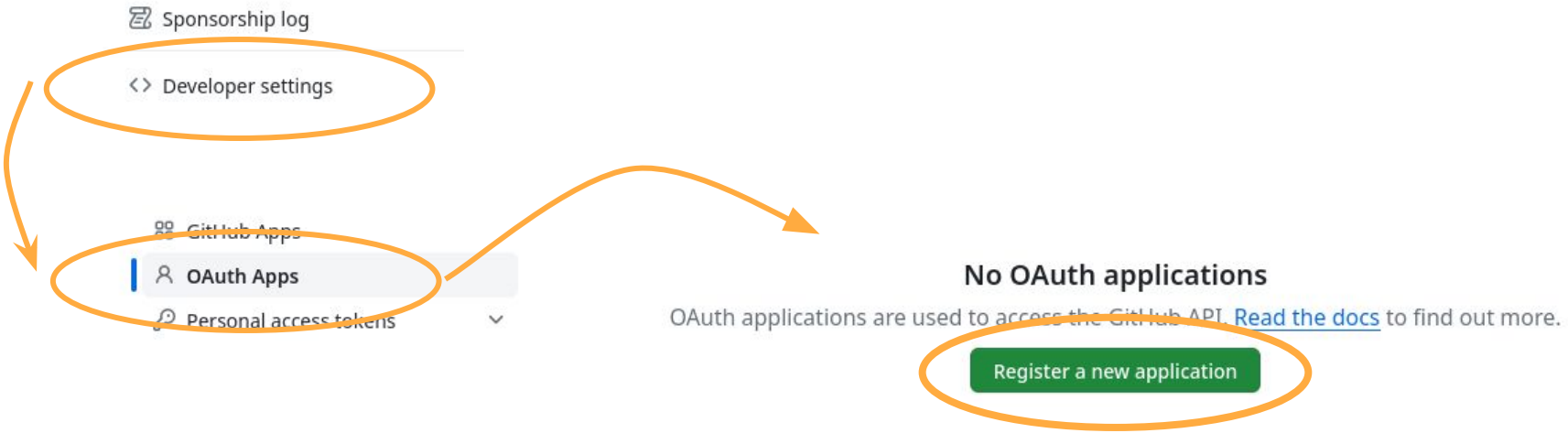


External IdP (Web SSO)

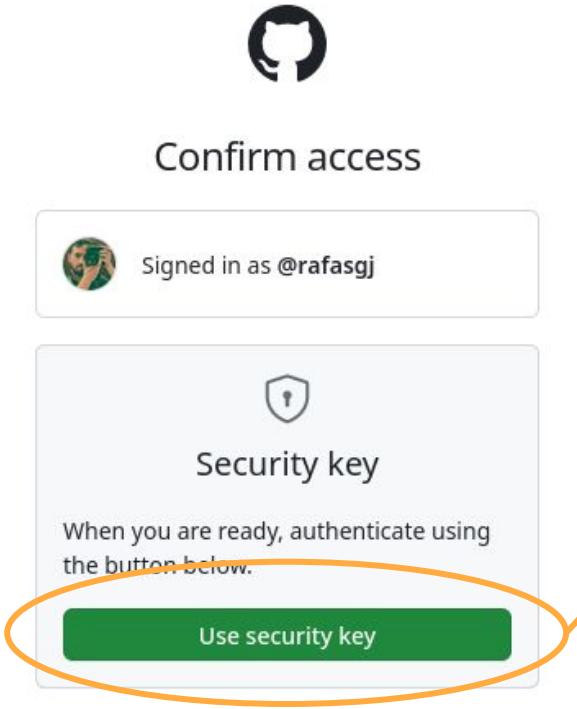


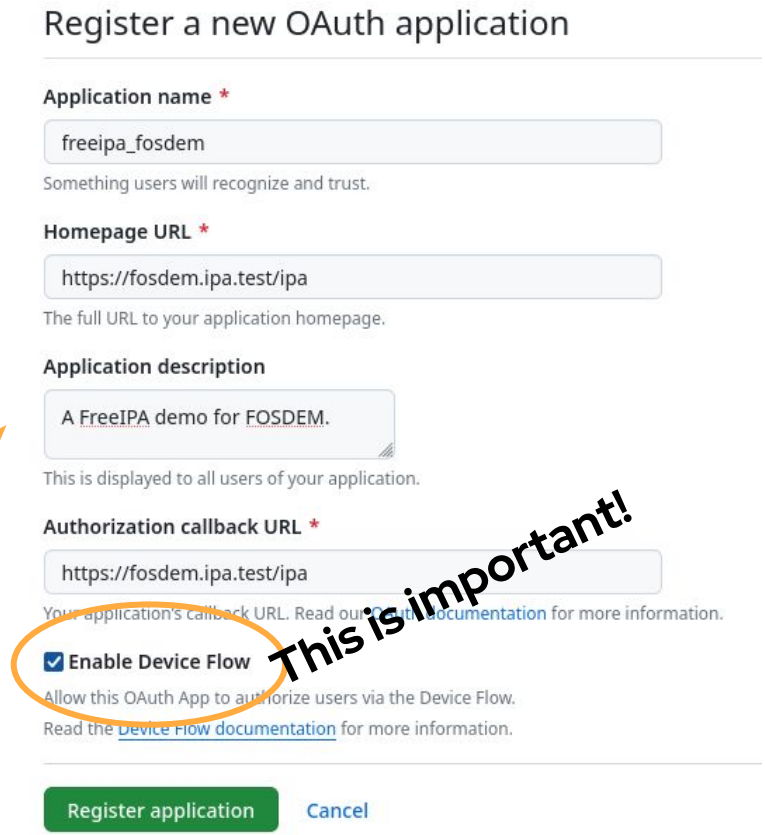
From FreeIPA external IdP design document:
https://freeipa.readthedocs.io/en/latest/designs/external-idp/external-idp.html

External IdP - GitHub example

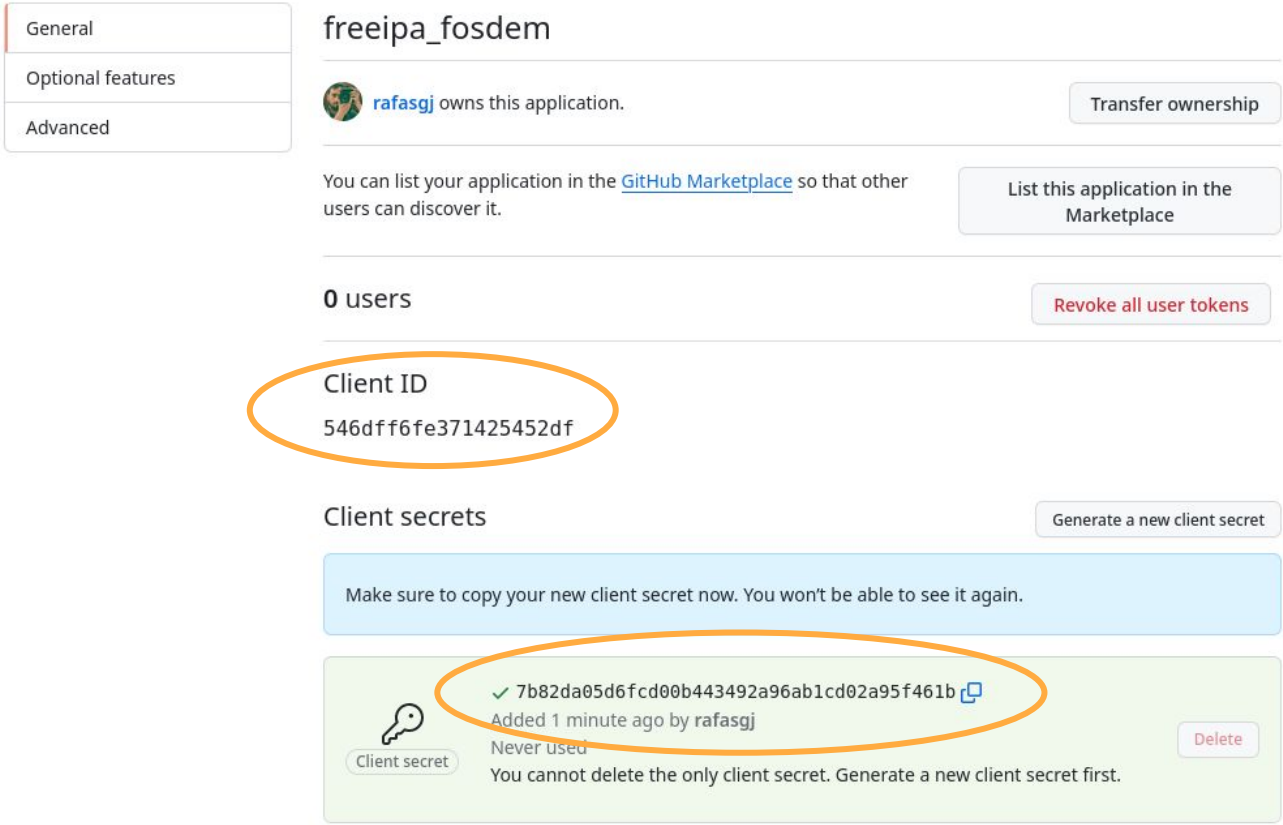


External IdP - GitHub example

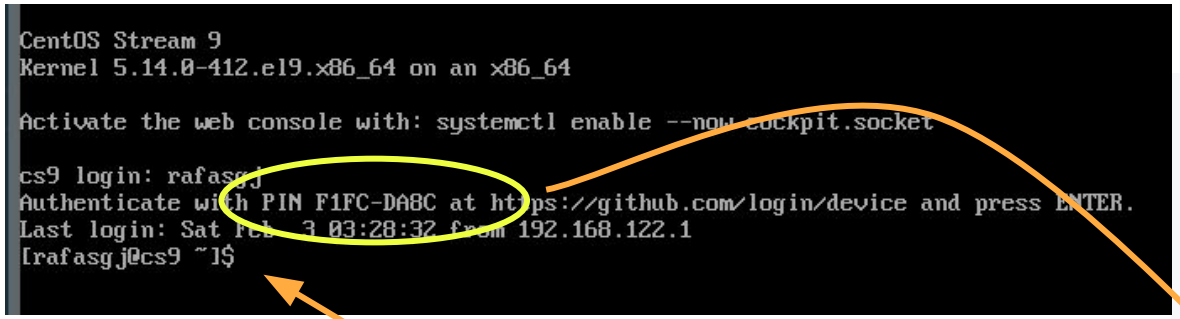


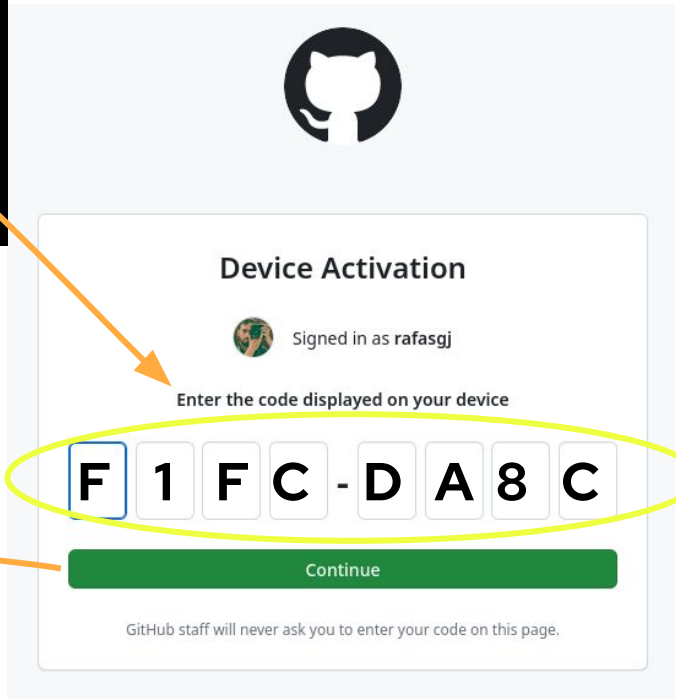


External IdP - GitHub example



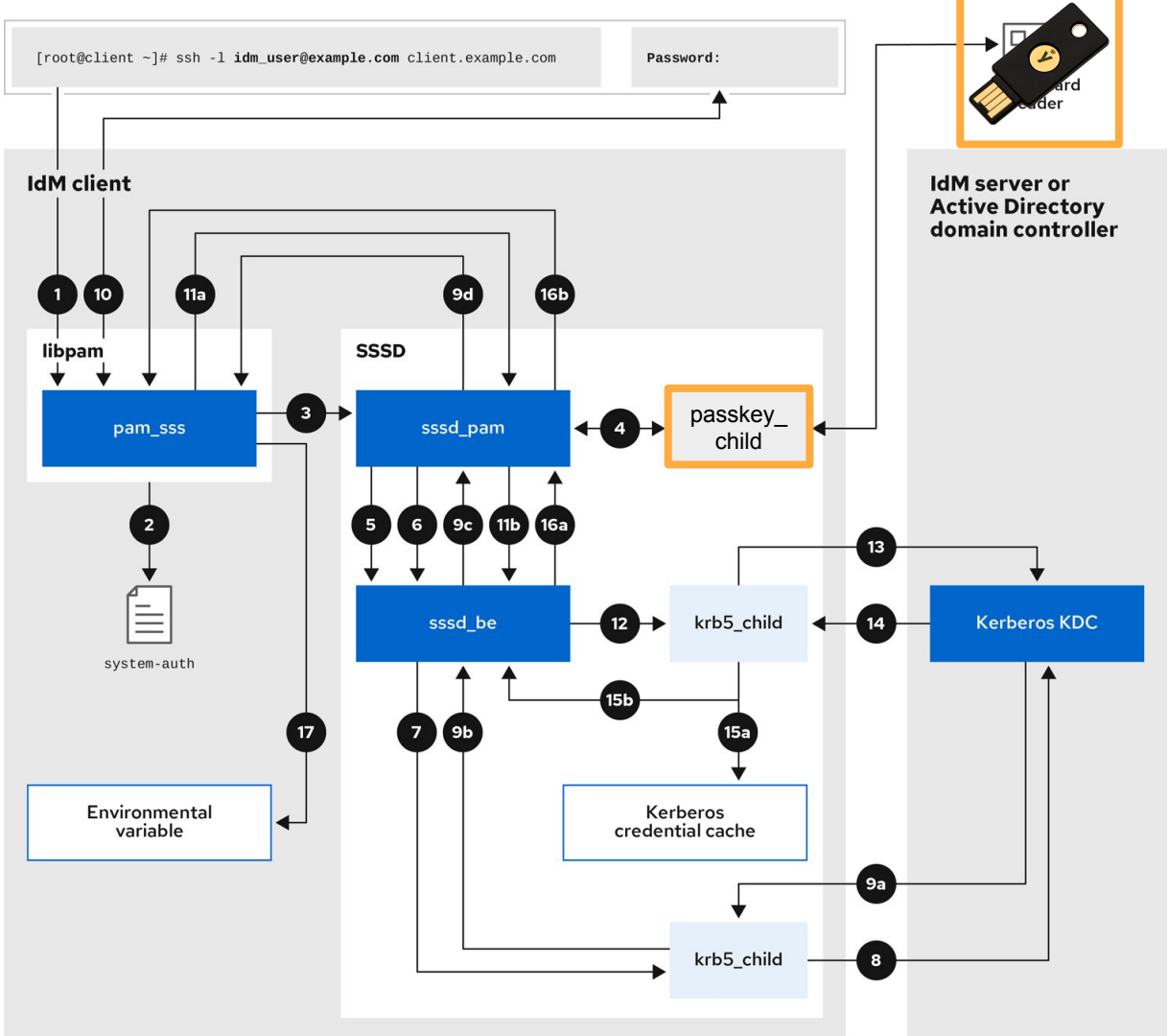
External IdP - authentication example





Passkeys

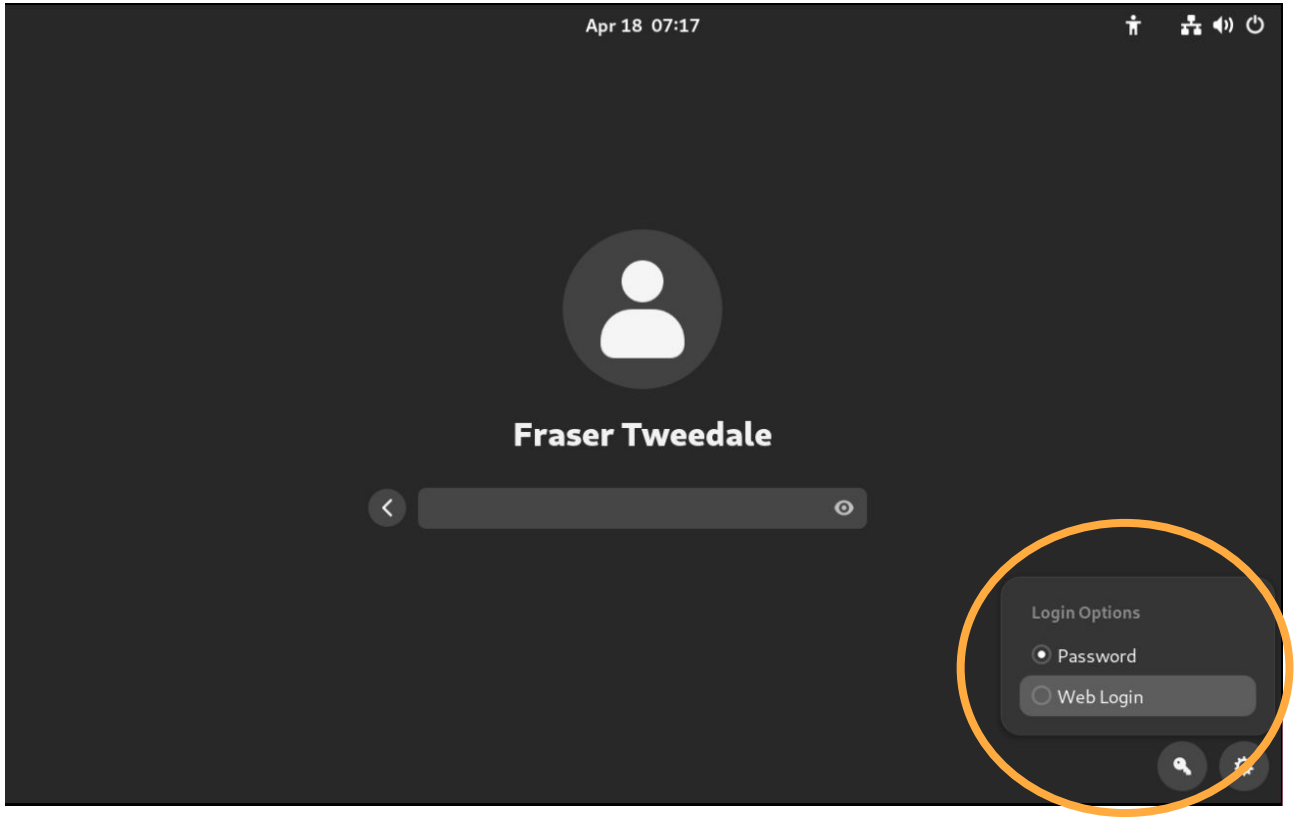
Diagram from RHEL guide *'Configuring and managing Identity Management'*: [8.3. Data flow when authenticating as a user with SSSD in IdM]



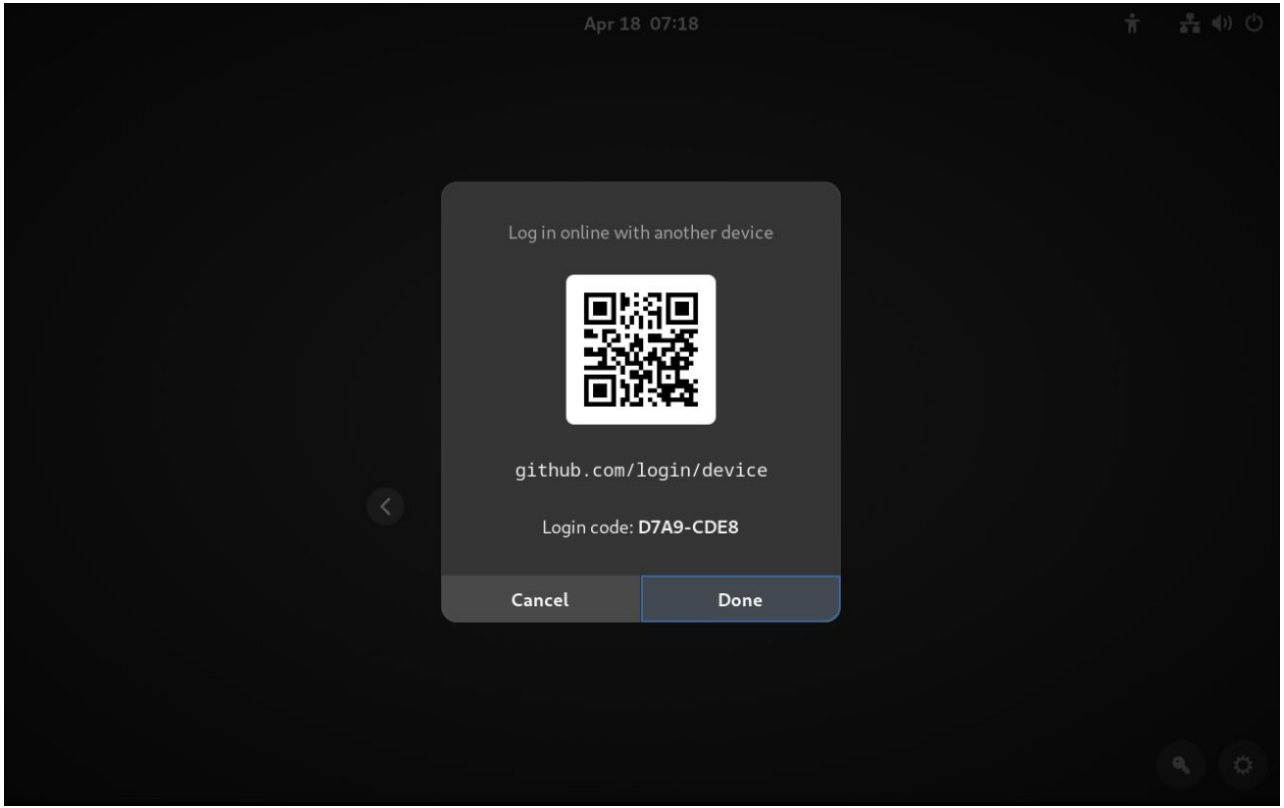
Passkeys

- `$ ipa user-add-passkey alice --register`
- `ipapasskey: passkey:9S87qLk8/RxYJ3skwwYduomAM+/HDtz...`
- Article: FIDO2 for centrally managed users - Fedora Magazine
- FreeIPA design page (link)
- SSSD design page (link)

GDM - mechanism selection



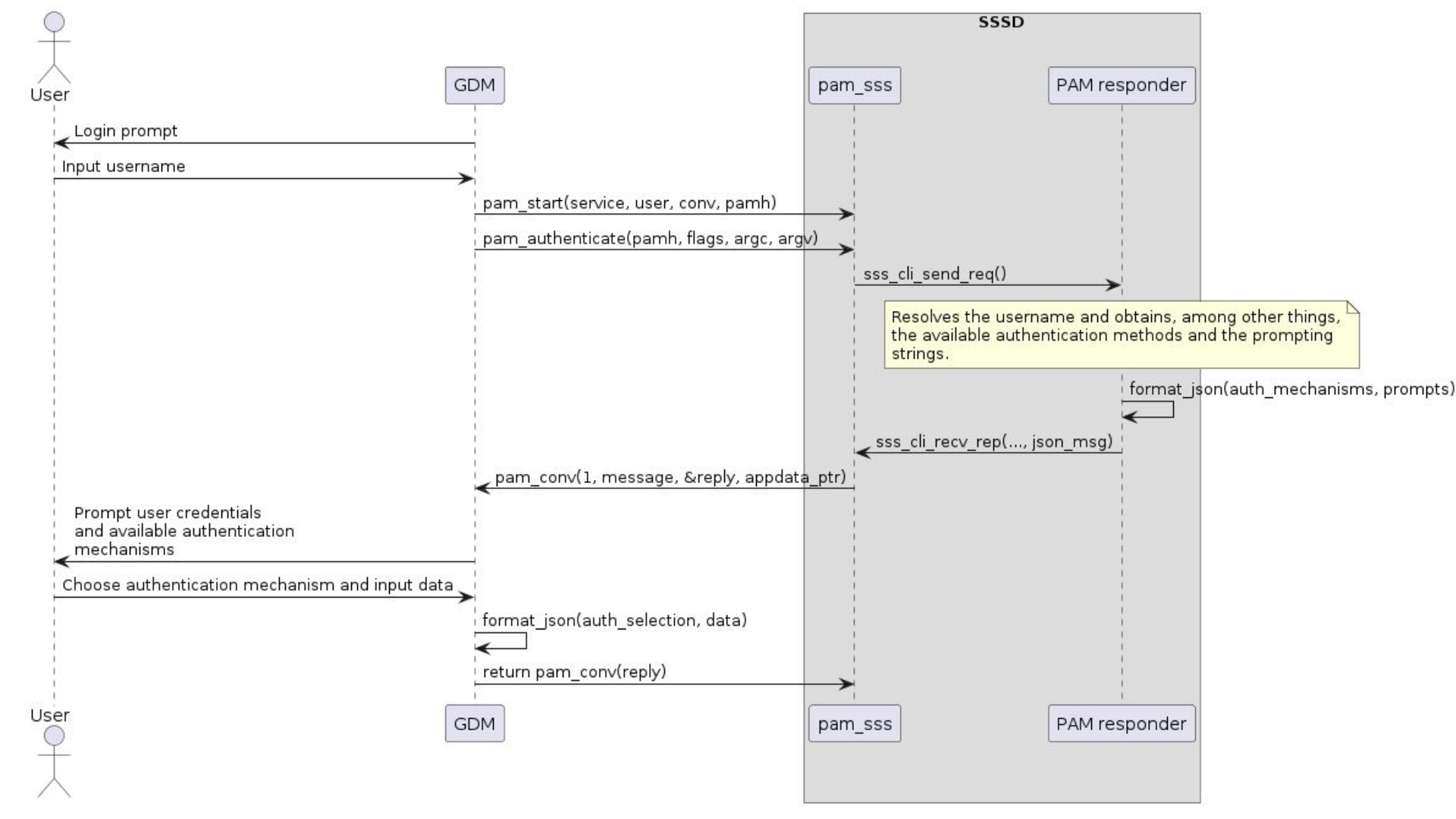
GDM - mechanism selection - External IdP



GDM - mechanism selection - UX

- GNOME UX research and mockups (link)
- SSSD design document (link)
- Development builds: **COPR** ipedrosa/passwordles-gdm
- To enable
  - Add to **/etc/sssd/sssd.conf**:

    ```
    [pam]
    pam_json_services = gdm-switchable-auth
    ```
  - **setenforce 0** *(temporary workaround)*
  - **systemctl restart sssd gdm**


SSSD
User
GDM
pam_sss
PAM responder
Login prompt
Input username
pam_start(service, user, conv, pamh)
pam_authenticate(pamh, flags, argc, argv)
sss_cli_send_req()
Resolves the username and obtains, among other things, the available authentication methods and the prompting strings.
format_json(auth_mechanisms, prompts)
sss_cli_recv_rep(..., json_msg)
pam_conv(1, message, &reply, appdata_ptr)
Prompt user credentials and available authentication mechanisms
Choose authentication mechanism and input data
format_json(auth_selection, data)
return pam_conv(reply)
User
GDM
pam_sss
PAM responder

GDM - mechanism selection

```
{
  "auth-selection": {
    "mechanisms": {
      "password": {
        "name": "Password", "role": "password", "selectable": true, "prompt": "Password:"
      },
      "eidp": {
        "name": "Web Login", "role": "eidp", "selectable": true,
        "init_prompt": "Login",
        "link_prompt": "Login online with another device",
        "uri": "https://short.url.com/tmp",
        "code": "1234"
      },
      "smartcard:1": {
        "name": "smartcard ID1", "role": "smartcard", "selectable": true, "prompt": "Enter PIN:"
      }
    },
    "priority": ["eidp", "smartcard:1", "password"]
  }
}
```

Availability

- **FIDO2** passkeys since SSSD 2.9.0 + **FreeIPA 4.11.0**
  - **Fedora 39**; RHEL 9.4 Beta (Technology Preview)
- **External IDP** since SSSD 2.7.0 + FreeIPA 4.10.1
  - Fedora 38; RHEL 9.1 (Technology Preview); **RHEL 9.4 Beta (full support)**
- **GDM** enhancements: ***not earlier than*** Fedora 41

Future

- **ipa-tuura** SCIM bridge - automatically CRUD external users/groups in IPA
  - https://github.com/freeipa/ipa-tuura
  - FOSDEM 2024 - *ipa-tuura: FreeIPA connector for Keycloak*
- **Stable POSIX attributes** for external IdPs
  - FOSDEM 2024 - *POSIX identities out of OAuth2 identity providers: how to redesign SSSD and Samba?*
- **Direct enrolment** to external IdPs
  - Cut out the middle man and run a **local KDC**: Web Login without FreeIPA
  - **Drop-in configuration** for pre-defined realms
- **Automatic domain join** in cloud environments
  - github.com/podengo-project

What I'm working on!

Resources

- **FreeIPA workshop**: https://freeipa.readthedocs.io/en/latest/workshop.html
  - Unit 12: External IdP (no passkey module… yet!)
- **WebauthN talk**: *"Webauthn, Passkeys, and You - The Future of Authentication"* - William Brown (EO 2023)
- **Smart cards talk**: *"Kerberos PKINIT: what, why, and how (to break it)"* - Fraser Tweedale (EO 2023) / **slides**
- **OIDC talk**: *Identity 2.0: the what, why and how of social and federated login"* - Fraser Tweedale (PyConAU 2017) / **slides**
- GDM+SSSD **development builds**: ipedrosa/passwordles-gdm **COPR**

Questions?

this slide deck:
is.gd/**passwordsmustdie**

@hackuador[@functional.cafe]