SLAC 2024

Using FIDO2 tokens with centrally managed user accounts

Thorsten Scherf
Red Hat

Agenda

- Passwords and other authentication methods
- Fast Identity Online (FIDO) overview & Demo
- FIDO2 for POSIX users
- SSSD / FreeIPA
- FIDO2 integration FreeIPA/LDAP/Active Directory & Demo
- OpenSSH
- Roadmap

Why no Passwords?

Hard to do it right

- Weak and reuse of passwords
- Complexity / Rotation policies
- Password managers not widely used
- Data breaches
- Phishing

We need something different…

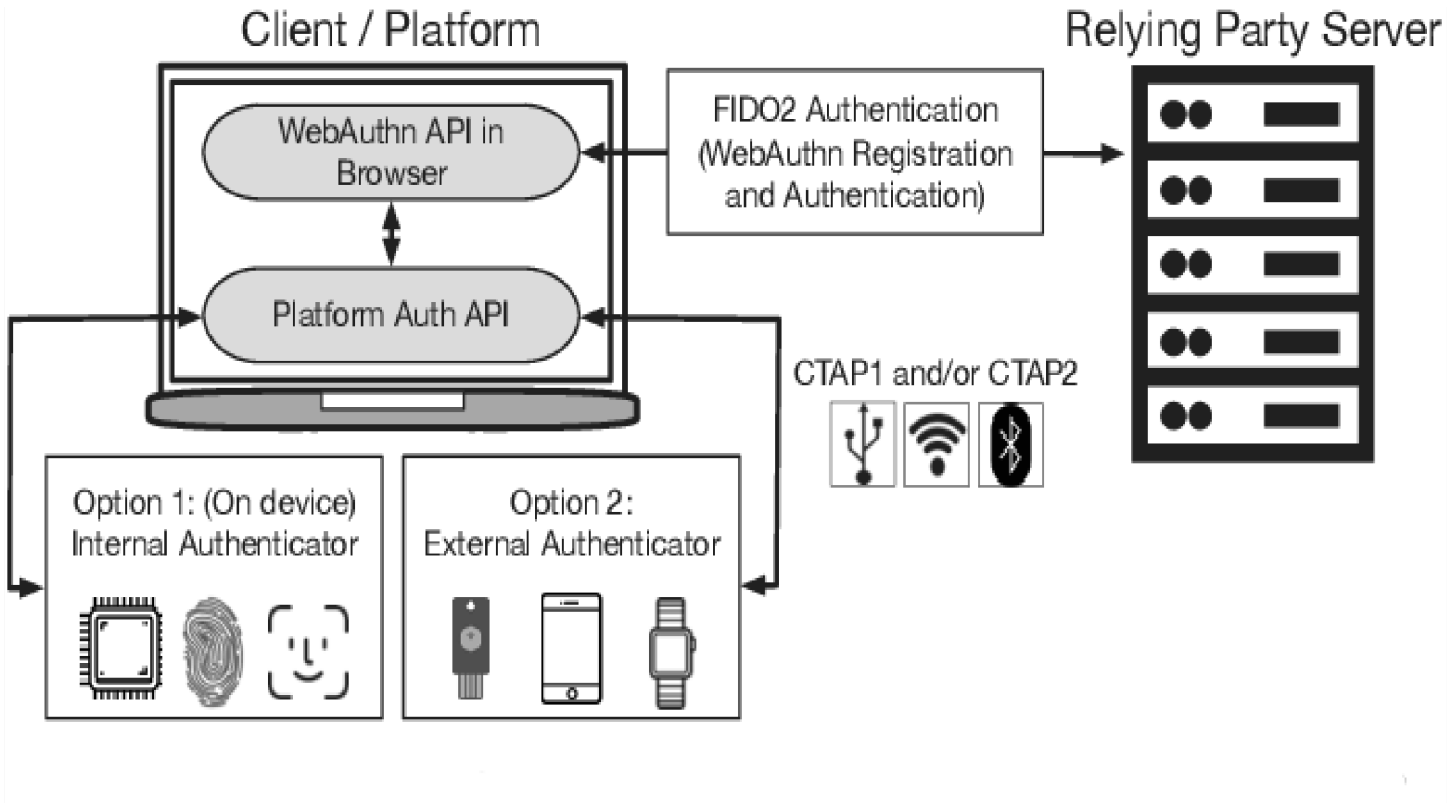
Password (only) alternatives

- 2FA, using HOTP or TOTP (phishable)
- Smartcards, using PKCS#11 tokens (phishing-resistant, but X.509)
- Web-SSO, using OAuth2 device authorization flow [1] (depends on external IdP and FreeIPA IdM)
- **FIDO2 / Passkeys** (phishing-resistant / good user experience)

1. https://www.heinlein-support.de/slac/2023/vortrag/freeipa-und-anbindung-externe-identity-provider

A bit of FIDO history

- FIDO1 (~2014)
  - U2F (Universal Second Factor)
  - UAF (Universal Authentication Framework)
- FIDO2 (~2015)
  - WebAuthn
  - CTAP2 (Client to Authenticator Protocol)
- Passkeys (~2022)
  - Based on FIDO2
  - Different implementations available
  - Many open questions



- Registration
- Authentication
- Discoverable Keys
- Non-Discoverable Keys

DEMO: WebAuthn

- https://webauthn.io/

Yubikey tools

- yubikey-manager
  - https://github.com/Yubico/yubikey-manager
- `$ ykman fido credential list`

```
Enter your PIN:
Credential ID  RP ID         Username  Display name
b868620c...    ssh:tuxgeek   openssh   openssh
2eab70dc...    example.com   pkuser
cfe842ba...    webauthn.io   tscherf
```

- Other FIDO2 devices
  - NitroKey, SoloKey v2, Token2, ...

FIDO2 for POSIX Users

- Key Registration
  - Key and mapping data stored in LDAP attribute (as part of user object)
- Authentication
  - Kerberos ticket issue (TGT)
  - Use SSO to connect to other services

Technologies

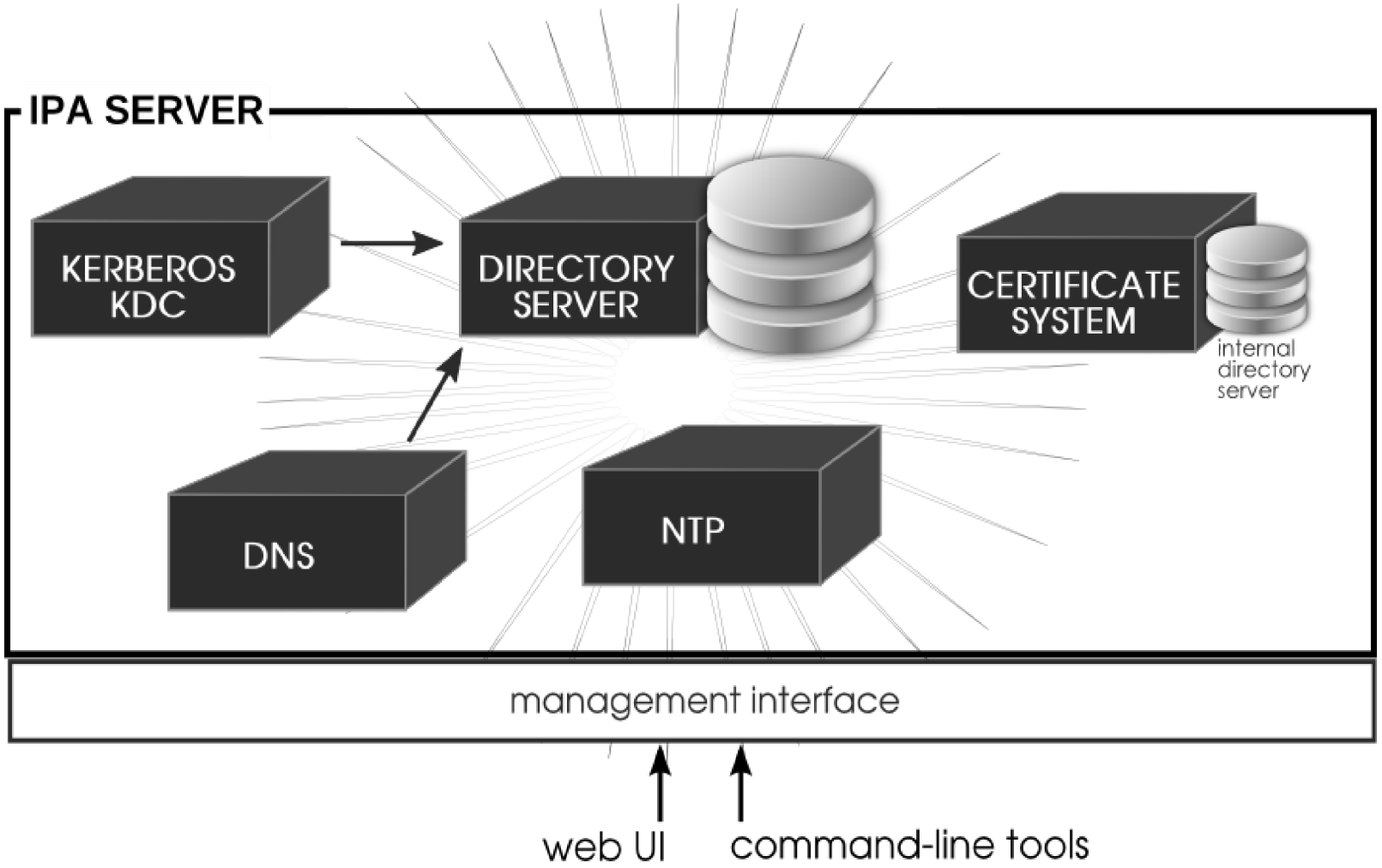
- System Security Services Daemon (SSSD)
- LDAP-Server (FreeIPA, Active-Directory, plain LDAP)
- Kerberos
- libfido2

What is SSSD?

- Open Source Client for Enterprise Identity Management
  - Enrollment of Linux systems into FreeIPA, Active Directory or LDAP domains
  - Uses remote identities, policies and various authentication and authorization mechanisms
  - Single PAM/NSS Module

What is FreeIPA?

- Identity Management solution
  - Provides centralized infrastructure to manage POSIX identities across a fleet of Linux machines
  - Combines 389-ds LDAP server, MIT Kerberos, SSSD, Samba, and Python-based management tools
  - Optionally also provides PKI and DNS services
  - Often seen as Active Directory for Linux


IPA SERVER
KERBEROS KDC
DIRECTORY SERVER
CERTIFICATE SYSTEM
internal directory server
DNS
NTP
management interface
web UI
command-line tools

LDAP attributes

- LDAP default attributes
  - `ipapasskey` (FreeIPA)
  - `altSecurityIdentities` (Active-Directory)
  - `passkey` (LDAP-Server)
- Non-default attribute names
  - `man 5 sssd-ldap-attributes`
- Attribute Format
  - `passkey:credentialId,pemPublicKey`

Key registration - FreeIPA backend

- New user

  ```
  $ ipa user-add USERNAME --first NAME --last SURNAME --user-auth-type=passkey
  ```

- Modify existing user

  ```
  $ ipa user-mod USERNAME --user-auth-type=passkey
  ```

- Device registration

  ```
  $ ipa user-add-passkey USERNAME --register
  ```

Key registration - LDAP- and Active-Directory backend

- Use sssctl tool

```
$ sssctl passkey-exec --register --username=USERNAME --domain=DOMAIN
```

- Generates the passkey and mapping data

```
passkey:oducHX2gU[...]sLlVf+j/d==,MFkwEwYHKo[...]fZ3+GM6h8g==
```

Key storage for LDAP- and Active-Directory backend

- Custom LDAP schema

```
attributeTypes: ( 2.16.840.1.113730.3.8.24.27 NAME 'passkey' DESC 'Passkey mapping' EQUALITY caseExactMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
objectclasses: ( 2.16.840.1.113730.3.8.24.9 NAME 'passkeyUser' DESC 'Passkey user' AUXILIARY MAY passkey)```
```

- Make sure your server knows about the updated schema

  `$ dsconf -D "cn=Directory Manager" localhost schema reload` (389DS)

- AD schema
  - Use default LDAP attribute `altSecurityIdentities`

SSSD configuration options

- `pam_passkey_auth`
- `passkey_verification`
- Other options available -> `man 5 sssd.conf`

DEMO: FIDO2 (Passkey) for POSIX Users

Availability

- SSSD-2.9.0 / FreeIPA-4.11.0
  - Fedora 39
  - Red Hat Enterprise Linux 9.4

Wait - what about OpenSSH?

- FIDO Support available since 8.2-ish
- OpenSSH uses different implementation
- ECDSA-SK and ED25519-SK crypto keys
- Not based on Linux PAM-Stack
- **SSSD users can use krb5 ticket to access SSH service**

Roadmap

- Attestation support
- GNOME integration (Auth-type selection, Online accounts, ...)
- Third-party tools integration
- Mobile phones

THANKS

tscherf@redhat.com