FedCA

Milan Sova, CESNET

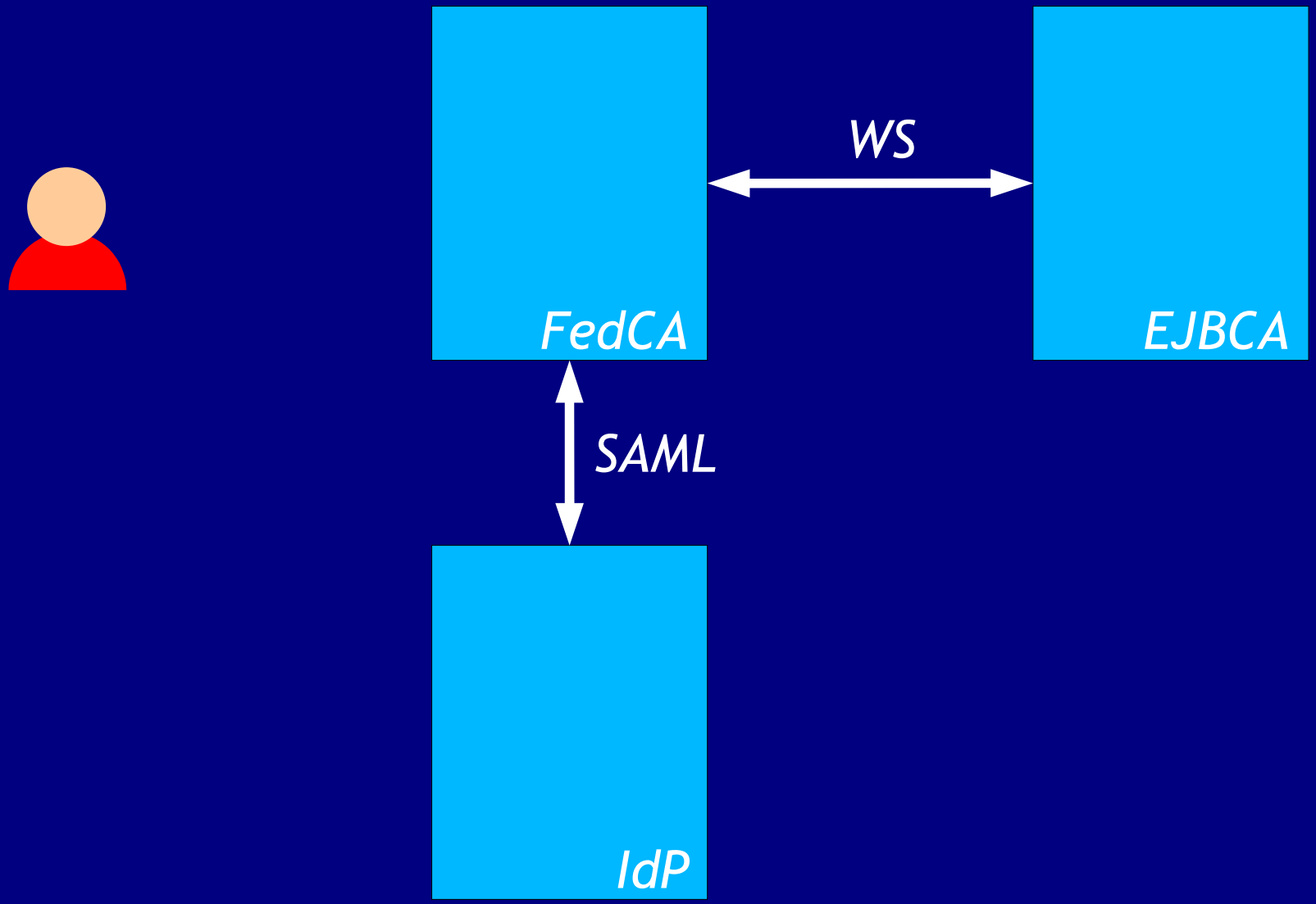
Requirements

- Full-fetured CA system
  - multiple CAs
  - separation of roles
  - web admin interface
  - HSM support
- open source
  - no licensing limits on # of certificates
- federable
  - convertible to an SP
  - out-of-band data into the cert

EJBCA

- open source (payed support optional)
- HSM
  - nCipher, Luna SA, PKCS11...
- web interface
  - admins authenticated with X.509 certs
- other interfaces
  - XKMS, CMP, SCEP, WS

Architecture



Attributes

- eduPerson**TargetedID**
  - key attribute
  - permanent
  - stored in the IdP directory

Authorizing attributes

- eduPerson**Entitlement**
  - one value per CA/[profile]
- optional
  - IdP
  - …

Naming attributes

- depend on the particular CA
- schacHomeOrganization
  - e. g. ***cesnet.cz***
- organization
  - e. g. ***CESNET***
- mail
- ...

Demo

Issues

- re-authentication
- logging of assertions (signed?)

ToDos & Plans

- HSM support
- cleaning the code & publishing

- “Smart” WAYF & Login (Shib2 reauth?)
- Implementing the “Classic” RA model

That's it