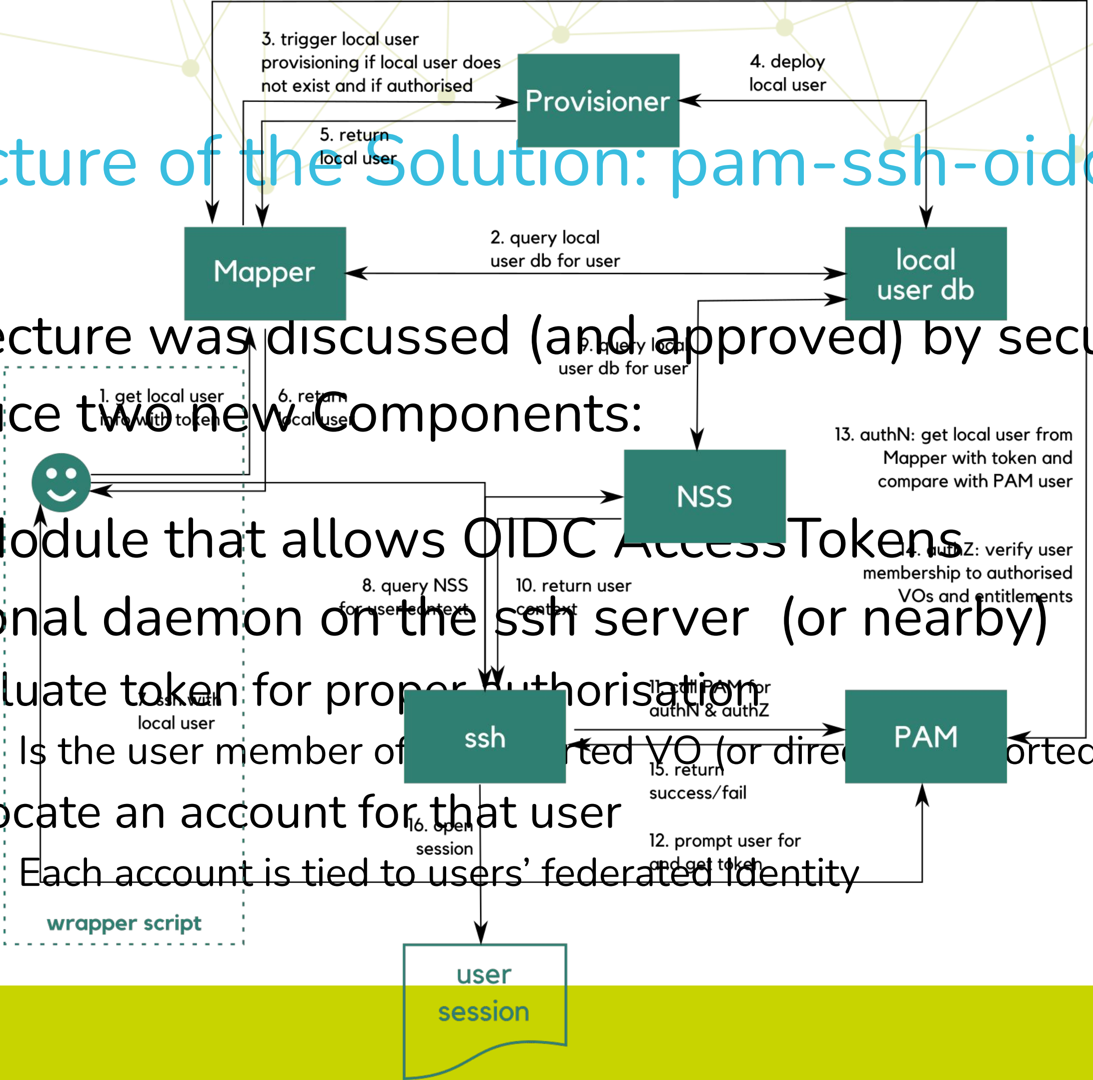
Access to HPC: SSH with OIDC

- Enable login to HPC (and VMs) with existing AAI
  - EGI **Check-in**, EUDAT **B2Access**, Geant: **eduTEAMS**, **HPB**, …
- Don’t modify **ssh** or **sshd**
- Straightforward authorisation model
  - Allow only members of supported Virtual Organisations
  - Allow authorised individual users
  - VOs are mapped to Unix Groups
- Traditional trust model
  - Grid: Cluster trusts VO-Server to authorise users
  - HPC: trusts PI to approve members of computing-project

Both are equivalent!

Architecture of the Solution: pam-ssh-oidc

- Architecture was discussed (and approved) by security experts
- Introduce two new Components:
- PAM Module that allows OIDC AccessTokens
- Additional daemon on the ssh server (or nearby)
  - Evaluate token for proper authorisation
    - Is the user member of a supported VO (or directly supported)
  - Allocate an account for that user
    - Each account is tied to users’ federated identity



Provisioner
Mapper
local user db
NSS
ssh
PAM
user session
wrapper script
1. get local user info with token
2. query local user db for user
3. trigger local user provisioning if local user does not exist and if authorised
4. deploy local user
5. return local user
6. return local user
7. ssh with local user
8. query NSS for user context
9. query local user db for user
10. return user context
11. call PAM for authN & authZ
12. prompt user for and get token
13. authN: get local user from Mapper with token and compare with PAM user
14. authZ: verify user membership to authorised VOs and entitlements
15. return success/fail
16. open session

Status

Packages (Beta test starting end May)

- Server:
  - PAM-Module: **pam-ssh-oidc** *debian,ubuntu,centos8,centos7*
  - Mapping Daemon **motley-cue** *debian,ubuntu,centos8*
- Client:
  - **oidc-agent + mc_ssh** . *Mac,debian,ubuntu,centos8,centos7*
  - **oidc-agent + (extended) putty** ..... *Windows (by end 2021)*

- Documentation: https://github.com/EOSC-synergy/pam-ssh-oidc
- Packages https://repo.data.kit.edu
- Contact: ssh-oidc@lists.kit.edu

Roadmap

- EOSC-Synergy Betatatest of deb+rpm packages => May 21
- Pooled accounts (grid-style) => June 21
- Final deb + rpm packages (client/server) for => July 21
- Tool for removing stale accounts (deprovisioning) => End 2021
- Windows support (patched putty, oidc-agent) => End 2021
- Mytoken support (non-expiring tokens)