OIDC support for SSH

Diana Gudu, Marcus Hardt, Gabriel Zachmann, Jonas Schmitt
Karlsruhe Institute of Technology

hardt@kit.edu
Motivation

- Enable federated access to shell-based services
  - Federated Identity Management → OpenID Connect (OIDC)
  - Shell-based services → Secure Shell (SSH), local identities

Our solution: server & client side tools
- Work with standard SSH software
- Use OIDC tokens for AuthN & AuthZ
- Manage local identities
Why would you use it?

...as a user

- Single Sign-On (SSO)
- No additional service credentials
- No need for SSH key management
- No prior registration
Why would you use it?

...as a service provider

- Benefits of federated AAI
  - Offload identity management to home organisation
  - Offload authorisation management to federation (VOs)

- Bridges the gap from federated to local identity
  - Manages the mapping of federated to local accounts
  - Manages the lifecycle of local accounts (create, update, suspend)
  - OIDC-based authentication → no need for managing additional credentials (passwords, ssh keys)
  - Manages access control based on federated authorisation models
Approach

- **Server side:**
  - Use PAM module with oidc support: `pam-ssh-oidc` (PSNC/Pracelab.pl)
  - Add REST interface to ssh-server to manage the details: `motley-cue`

- **Client side:**
  - `oidc-agent` for obtaining tokens
  - Enable `ssh-clients` to use tokens

No modifications of `ssh` or `sshd`
Server Side
motley-cue architecture

- REST API
  - /user
  - /admin
  - /verify_username

- Authorisation Layer
- Identity mapping
- Interface to local IAM

- PAM
- Local Identity Management
Authorisation

- Support for multiple OIDC Providers
- Based on VO membership
- Based on assurance
- Individual users via sub+iss
Local User Management

- Interface to site-local identity management systems
  - Extensible, plug-in architecture
  - Supported identity backends: UNIX accounts, LDAP, KIT RegApp

- Identity mapping: \texttt{sub + iss} $\rightarrow$ \texttt{local username}
  - Stored directly in the local IdM system
  - Username generation strategies $\rightarrow$ uniqueness
    - Friendly: preferred username, first_last, ...
    - Pooled: egi001, egi002, ...
  - VOs mapped to local groups
Advanced features

- Approval workflow → admins oversee all deployment requests
- LDAP backend → for managing local accounts
- Audience → restrict access to tokens released for configured audience
- Long tokens → 1kB too long for SSH, generate one-time tokens
Easy deployment
- Packages for most common Linux distributions
- systemd integration
- Python, FastAPI

Packages provided for major Operating Systems (that run sshd)

```
$ apt install motley-cue pam-ssh-oidc
$ vim /etc/motley_cue/motley_cue.conf
$ systemctl restart motley-cue
```

http://repo.data.kit.edu
Nice to know

- SSH daemon is not modified
- PAM module may be combined with other modules
  - Possible: ssh-key + password + OIDC + 2\textsuperscript{nd} factor (linotp)
Client Side
SSH Clients

- 2 Simple changes on the command line:
  - add our wrapper tool mccli
  - replace username with identity provider

  Old: `ssh marcus@ssh-oidc-demo.data.kit.edu`
  New: `mccli ssh ssh-oidc-demo.data.kit.edu --oidc egi`

- Tools to install:
  - `$ pip install mccli`
  - `$ apt-get install oidc-agent`

- Again: packages provided for all major Operating Systems

http://repo.data.kit.edu
SSH Clients

- Everything is different on Windows ;)
- Putty SSH Client required source code modifications
  - Joint effort with Simon Tatham (putty main developer)
  - General Plugin Interface (available in putty-0.78: [https://www.chiark.greenend.org.uk/~sgtatham/putty/prerel.html](https://www.chiark.greenend.org.uk/~sgtatham/putty/prerel.html))
- Plugin and oidc-agent installed and shipped together
  [http://repo.data.kit.edu/windows/oidc-agent](http://repo.data.kit.edu/windows/oidc-agent)
Recorded Demo

- This demo shows the first-time setup on windows
- Choices are cached. User only enters password **once** (for each windows reboot)
Live Demos

- 1. Usage from linux
- 2. Usage from windows
Live Demo Server
for You to try this

https://ssh-oidc-demo.data.kit.edu/
Contributors

- **PAM module (pam-ssh-oidc):** Pracelab.PL (Pawel Wolniewicz (PSNC), Damian Kaliszan (PSNC))
- **User provisioning (feudal):** KIT (Lukas Burgey, Joshua Bachmeier, Diana Gudu, Marcus Hardt)
- **Integration serverside (motley_cue):** HIFIS (Diana Gudu (KIT), Andreas Klotz (HZB))
- **HPC Integration and testing:** EOSC-Synergy (Diana Gudu (KIT), Rubén Díez, CESGA)
- **Integration, consulting, and review:** Enol Fernandez (EGI), Viet Tran (IISAS), Mario David (LIP), Mischa Salle (Nikhef)
- **Infrastructure Manager Integration:** Miguel Cabeller (UPV), German Molto (UPV)
- **oidc-agent integration:** KIT (Gabriel Zachmann (KIT))
- **putty-integration:** Dmytro Dehtyarov (KIT/GEANT), Jonas Schmitt (KIT), Simon Tatham (Putty), Niels van Dijk (SURFnet)
More information

- Download oidc-agent for Windows & PuTTY
  [QR code](https://repo.data.kit.edu/windows/oidc-agent)

- Demo server
  [QR code](https://ssh-oidc-demo.data.kit.edu/)

- Contact
  m-contact@lists.kit.edu