# Automating dCache monitoring test transfers with OIDC tokens using Mytoken

Karlsruhe Institute of Technology (KIT)
Scientific Computing Center (SCC)
Scientific Data Management (SDM)

1. Motivation
2. Outset
3. Main Obstacles
4. Candidate OIDC Agents
5. Switch to Mytoken

# Motivation

1. WLCG decided to retire X.509 and Globus and transition over to bearer tokens following the WLCG JWT Profile
2. AuthN and AuthZ handled by OIDC providers, which dCache (blindly) trusts
3. Major problem: Token facilities are designed for breathing individuals and short, precise use-cases
4. What about continuous, automated scenarios, like monitoring?

# Outset - References

- Automation of OIDC Token Management foundation for this slide show
- Using OpenID Connect with dCache in The Book (v10.2)
- Understanding Macaroons in dCache User Guide (v10.2) Chapter 1
- OIDC tokens for beginners by Onno Z., 18th dCache WS
- OIDC and all that Jazz by Marina S., 17th dCache WS
- dCache Frontend OIDC authentication using Keycloak as Identity Provider by Elena P., 16th dCache WS
- WLCG Common JWT Profiles, v1 09/25/2019
- Mytoken homepage
- OpenID Foundation
- OIDC Terminology
- OpenID Authentication 2.0 specification
- JSON Web Token (JWT) RFC

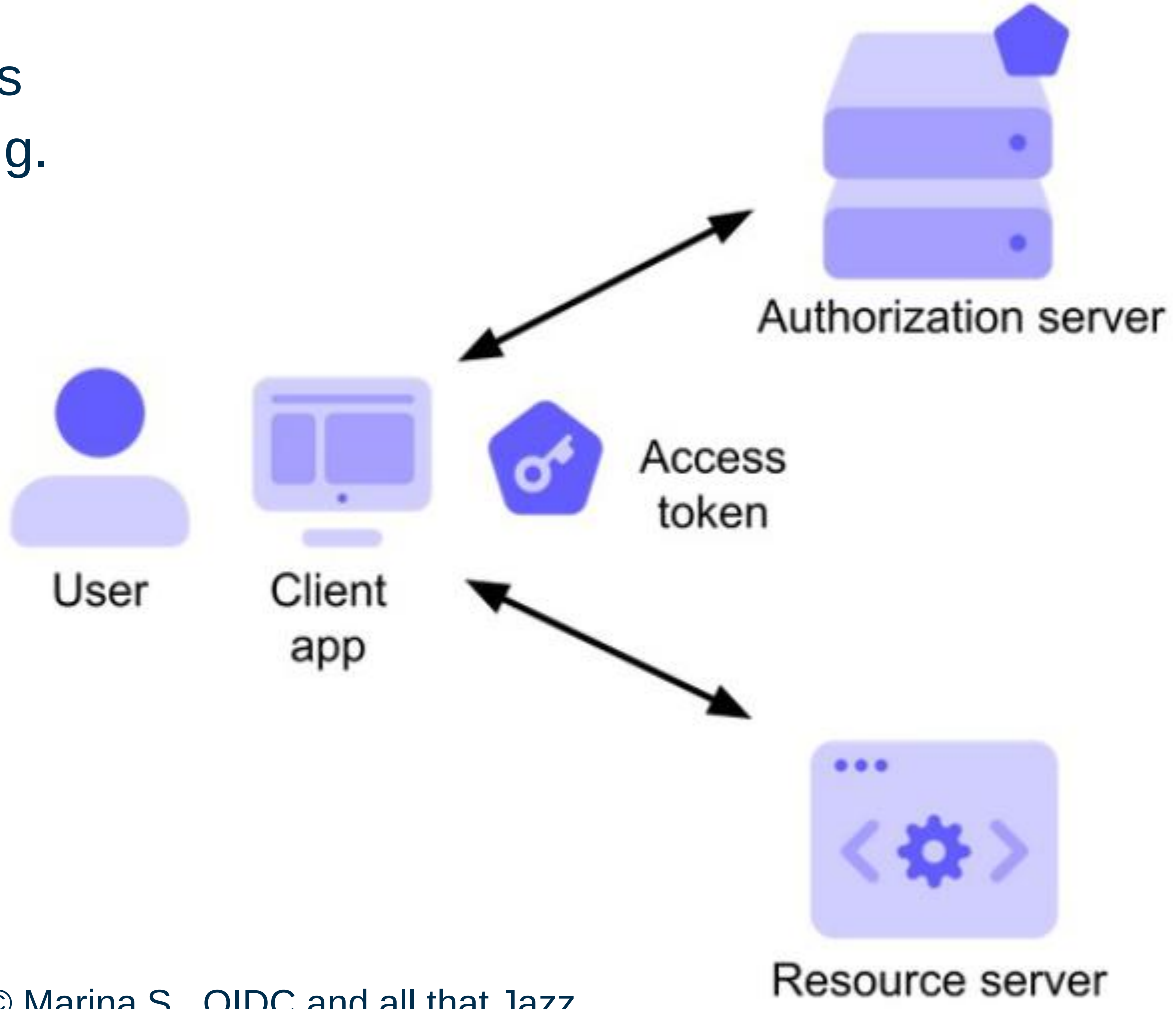
# Outset - Terminology (used in these slides)

| Acronym | Full Term | Explaination |
|---|---|---|
| OP | OIDC Provider | "OAuth 2.0 Authorization Server that is capable of Authenticating the End-User and providing Claims to a Relying Party about the Authentication event and the End-User." |
| AT | Access Token | "Access tokens are credentials used to access protected resources." |
| RT | Refresh Token | "Refresh tokens are credentials used to obtain access tokens." |
| MT | Mytoken Token | Type of Bearer Token developed to provide ATs to long-running compute jobs. |
| IAM | Identity and Access Management | "IAM is a framework of policies and technologies to ensure that the right users […] have the appropriate access to technology resources." |

# Main Obstacles

1. Users obtain ATs from IAM as OP with preferred apps
   - User must pass **interactive challenge** (through e.g. web browser) as *essential security feature*
2. ATs enable access to *protected resources*

- ATs expire quickly (max 6 h in WLCG)!
- RTs authorize retrieval of fresh ATs w/o repeated authentication
- **RTs expire** (max 30 d in WLCG)!

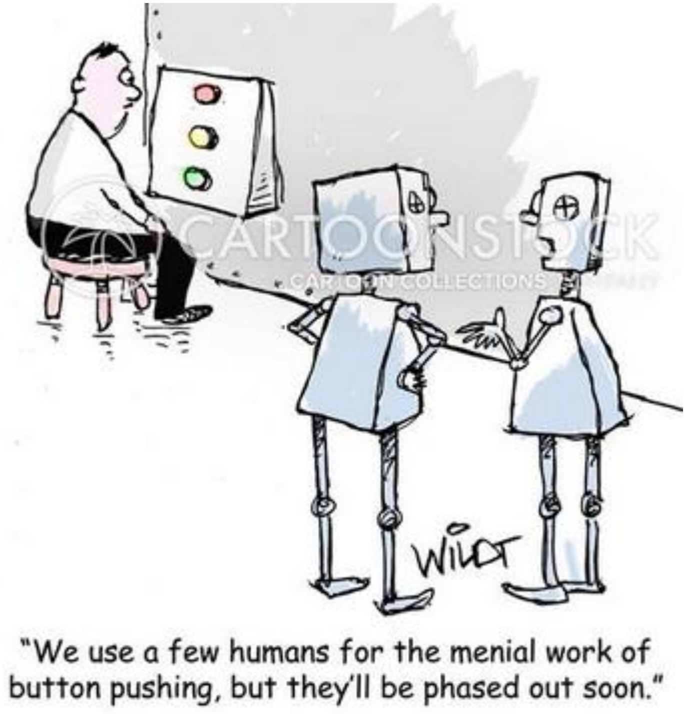


© Marina S., OIDC and all that Jazz

# Main Obstacles – Solutions?

## A

- Somebody needs to manually refresh RTs
  - Unreliable and tedious for continuous scenarios



"We use a few humans for the menial work of button pushing, but they'll be phased out soon."

## B

- Work around interactive challenge process
  - If that was possible, then OIDC is flawed

## C

- Establish Trust Relationships

# Candidate OIDC Agents – `oidc-agent` (Solution A)

- `oidc-agent` designed like `ssh-agent`
  - Handle OIDC tokens like ssh-keys
- Daemon w/o systemd integration, needs supplementary agent service per user session
- Generate accounts with OPs using `oidc-gen`
  - This is one **interactive challenge**
- Request ATs explicitly for known OPs only with `oidc-token`
- `oidc-agent` is integrated with other applications

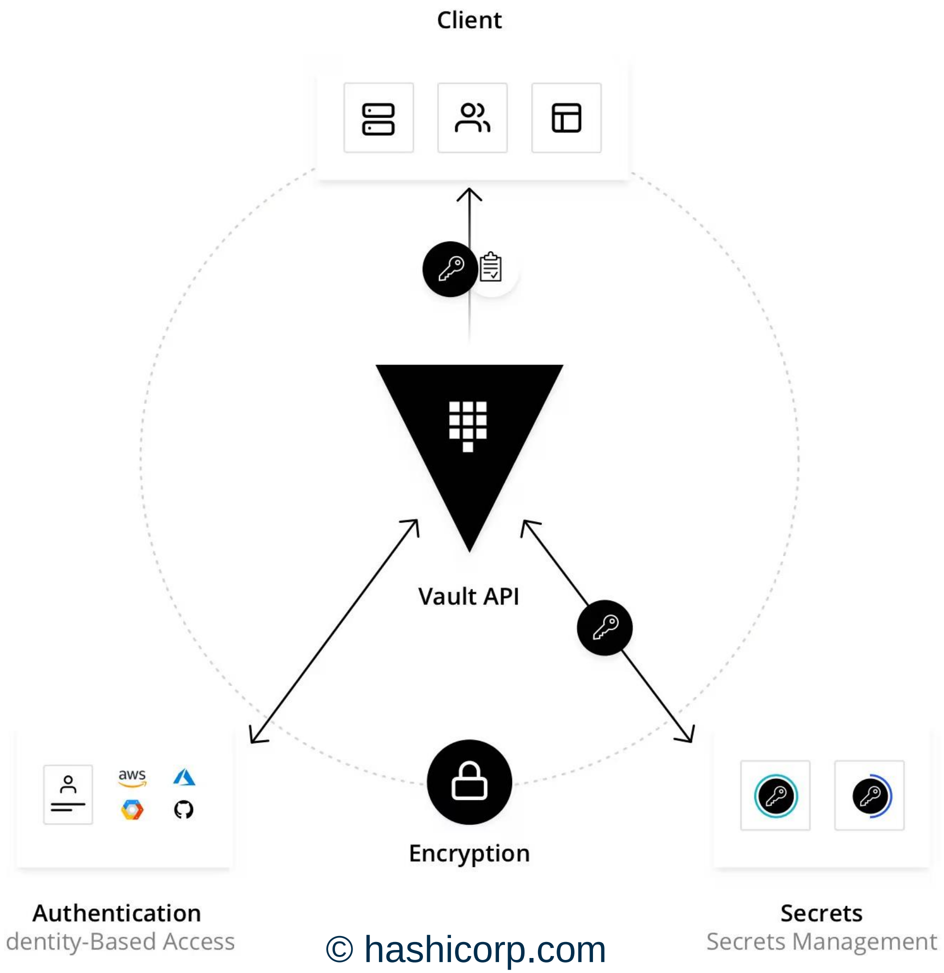
# Candidate OIDC-Agents – `osg-token-renewer` (Solution A)

- `osg-token-renewer` builds on top of `oidc-agent`
- systemd-integrated timer replacing tokens periodically
- Requires **initial interactive** setup of client accounts
- Stores credentials on disk, in order to refresh tokens

# Candidate OIDC-Agents – Hashicorp Vault (Solution C)

- Using Hashicorp Vault as a Service for Managing Tokens by Dave D., WLCG Grid Deployment Board 2021

- Integrated with HTCondor
- `condor_submit` uses Vault Tokens (VT) to fetch ATs on behalf of a user
- ATs are bound to jobs, which access resources
- Vault stores RTs per OP
- Vault admins can create indefinitely renewable VTs for unattended operations
- Requires trust between Vault and OP



© hashicorp.com

# Candidate OIDC-Agents – Mytoken (Solution C)

- Developed by same team as `oidc-agent` at KIT
- Designed explicitly for unattended, long-running tasks
- Mytoken server mediator between user/robot and OP
  - Client submits MT to Mytoken server
  - Mytoken server fetches AT from OP
  - Mytoken server may enforce restrictions on MTs (e.g. dates, requester IP address or geo-location)
  - MTs are transferrable
- Mytoken server supports generic clients:
  - `mytoken` client tool, `curl` and `oidc-agent`
- MTs and ATs need to be managed by clients
- Requires trust between Mytoken server and OP

# Switch to Mytoken

- Select Mytoken for its simplicity and low barrier to entry
  - Hashicorp Vault more flexible, but too much overhead for use-case (monitoring)
  - Mytoken provides features mitigating compromises regarding RT handling
- Convince CERN dteam IAM admins to trust public mytok.eu instance as OIDC client
  - mytok.eu can now cooperate with CERN dteam IAM and retrieve immortal RTs*
  - All MTs and ATs produced by mytok.eu and CERN dteam IAM as OP are *limited to dteam VO*, which is explicitly dedicated to development, testing and monitoring anyway
- Any other WLCG site is invited to utilize this service – no further agreements necessary

*) AARC-G081 suggests to limit the lifetime of RTs to at most 1 year. mytok.eu is committed to implement a robust and versatile notification system, which will raise attention towards dying RTs or other imortant events, like abuse of MTs.

# Switch to Mytoken

- Get your AT with MT via command line

```
$ /usr/bin/mytoken AT --MT-file /path/to/MT --out /path/to/AT \
    -s storage.read:/ -s storage.stage:/ -s storage.create:/ -s storage.modify:/
$ BEARER_TOKEN_FILE=/path/to/AT
$ BEARER_TOKEN="$(cat /path_to_AT)"
```

- These two environment variables feed into the WLCG token discovery
  - Alternatively, `oidc-tokensh` – the equivalent to `httokensh` developed at FNAL – will ensure that new ATs are stored at `/tmp/bt_u${id -u}`
- Same old scripts running test transfers should work out-of-the-box and prioritize discovered tokens
  - If transfers fail using tokens, client tools may fall back to traditional VOMS proxies

# Questions?