Fermilab | U.S. DEPARTMENT OF ENERGY | Office of Science

Token-based AAI at Fermilab

Jeny Teheran

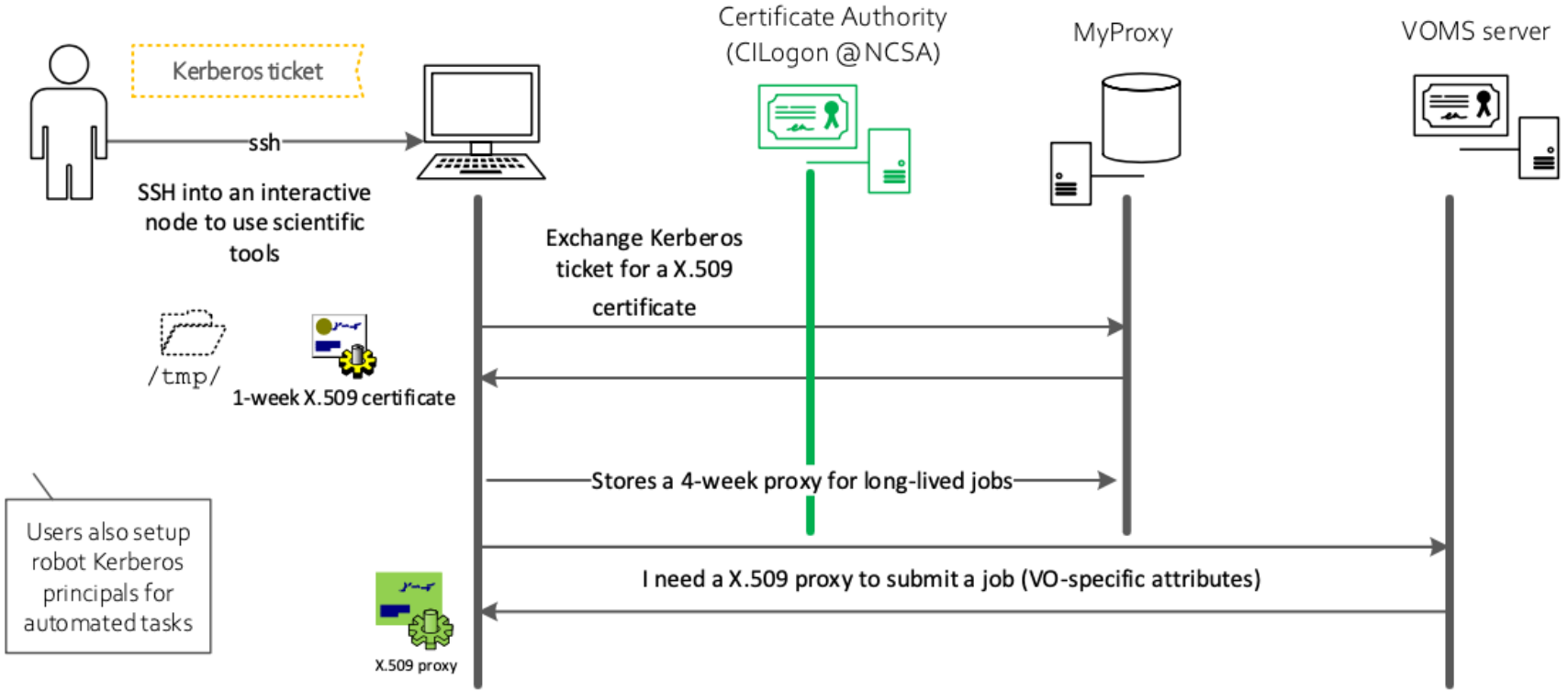
Internet2 Technology Exchange 2022

6 Dec 2022

Context

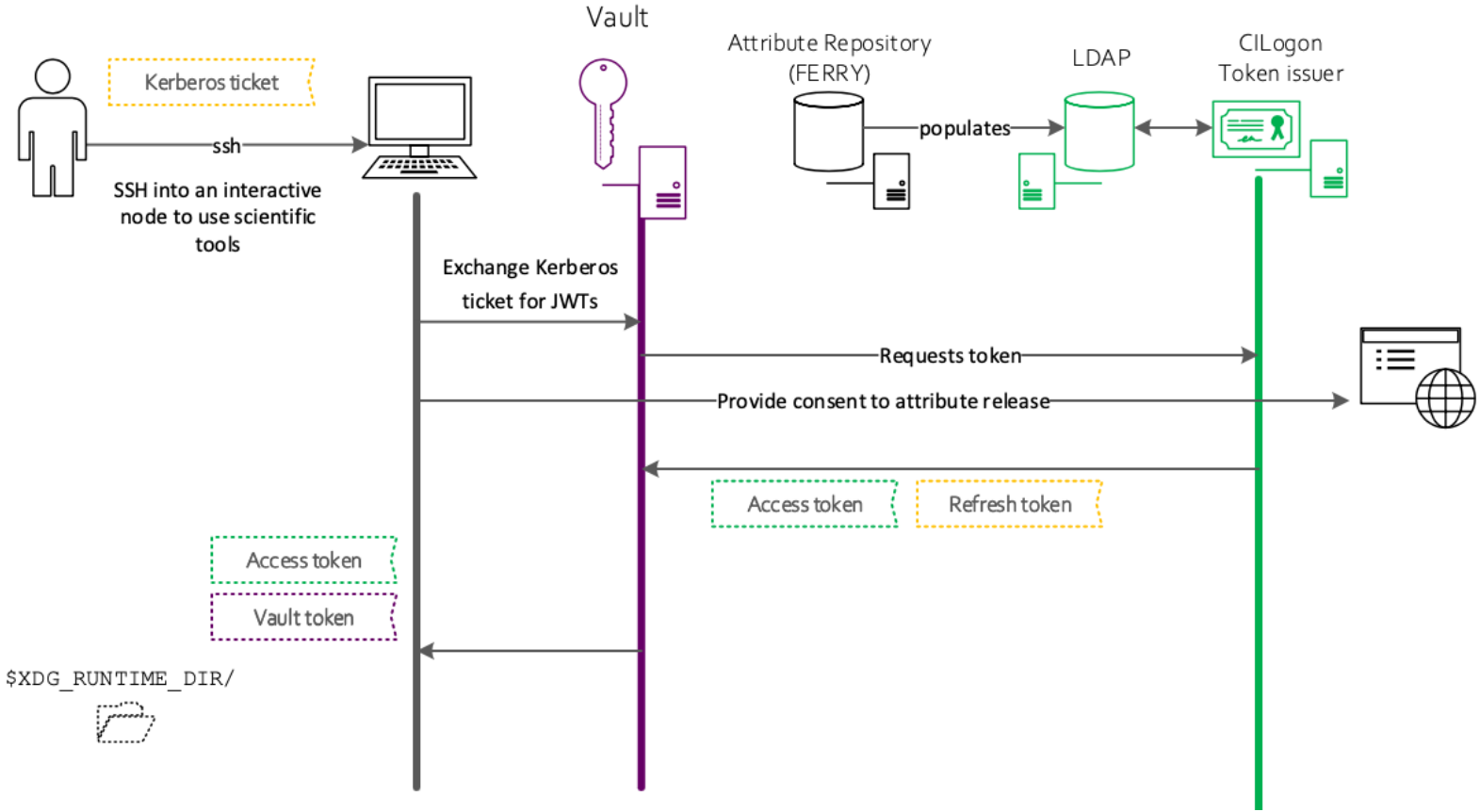
- Fermilab provides shared scientific services for multiple VOs:
  - Largest T1 for CMS in the US
  - Non-LHC, small VOs such as NOvA, Muon g-2 (neutrino experiments).
  - Larger VOS and international collaborations like DUNE: Deep Underground Neutrino Experiment.
- Our environment for scientific services and tools is command-line oriented.
- Goal → Align our authentication and authorization infrastructure with current technologies:
  - Reduce complexity on the authentication infrastructure by moving away from X.509 user certificates towards industry-standard technologies such as OAuth, OIDC and JWT.
  - Guarantee interoperability for international collaborations moving towards token-based AAI, such as CMS.

Transitioning to tokens: current infrastructure



Fermilab

Transitioning to token: Token-based AAI



Fermilab

Current Status

- New components:
  - `htgettoken` is a new general-purpose script tool for user interaction with Vault. Replaces cigetcert.
  - Hashicorp Vault as OIDC client: replaces MyProxy in our architecture; HTCondor reads tokens for long-lived jobs from it.
- FERRY database (contains authorization attributes) is exported to an LDAP instance hosted at CILogon.
- The OIDC token issuer at CILogon make its decisions based on the information populated in LDAP:
  - Separate token issuers for international collaborations (VOS) and a shared Token issuer for smaller VOs

Challenges 1/2

- Integrating token-support into a diverse set of batch management and data transfer tools.

- Multiple token issuers: VOs like DUNE get their own Token issuer. Smaller VOs share a token issuer for Fermilab (as an umbrella VO):
  - "`iss`" claim is the same token issuer URL, where to include the subVO?

```
SCITOKENS /^https:\/\/cilogon.org\/dune,.*/ dunepro
SCITOKENS /^https:\/\/cilogon.org\/dune,.*/ dunecal
```

Same issuer, different roles hence different capabilities and mapping.

Challenges 2/2

- Operating a hybrid environment while enabling experiments data taking and processing schedules:
  - DUNE has not started yet, but simulations and smaller-scale experimental projects like ProtoDUNE have strict schedules for data processing.
  - Before transition is completed across the global infrastructure, user jobs will require both credentials: X.509 proxy cert and access token

Future plans and concerns 1/2

- As Fermilab becomes the host laboratory for international collaborations like DUNE, it is our goal to provide transparent access to computing resources for all of our scientific user community across organizational and national boundaries.
  - There are simpler use cases than job submission and data transfer that can be easily supported by expanding our federation project.

Future plans and concerns 2/2

- The issue of Trust and Cybersecurity:
  - A subset of NIST CSF cannot be directly applied to scientific computing resources.
  - Instead, we rely on compensatory controls mainly based on trust:
    - Protect our resources from cyberattacks enabling reproducible and trustworthy research
    - Establish acceptable risks levels while operating our computing infrastructure.
- "*IGTF is uniquely positioned to help in building trust in the R&E community*"
- "*Trust is earned by sharing common policies and practices, and is sustained by behaving reliably within a community of practitioners, on behalf of relying parties*"
- M-22-09 Federal Zero Trust Strategy: we don't know yet the impact of ZTA in our cybersecurity posture and controls.

D. Simmel. TAGPMA/IGTF activities in trust of attribute authorities. 16th FIM4R and TAGPMA. Internet2 TechEx 2022.

1. User experience remains a priority: convenient access is key to enable science

2. Our community of experts (WGs, committees, taskforces) is our main advantage.

3. Our cybersecurity landscape changes and so should we.

Jeny Teheran, Cybersecurity Architect

Email: jteheran@fnal.gov

https://www.linkedin.com/in/jenyteheran/