Authorization and Authentication Evolution: Leaving the identity behind

MORGRIDGE
INSTITUTE FOR RESEARCH
RESEARCH COMPUTING

FEARLESS SCIENCE

Authorization and Authentication Evolution

Two major changes are occurring in the global Authentication and Authorization Infrastructures (AAI) used by HEP:

1. Movement toward using standard tooling and broad, global infrastructure(s) for AAI.
2. Pushing "identity" from the center to the edges of the distributed system.

Migrating away from GSI

HEP uses infrastructures - such as OSG, EGI, and WLCG - to meet its AAI needs. Traditionally, the AAI was built on the foundation of the "Grid Security Infrastructure" (GSI). GSI components include:

1. Base of X.509-based PKI used by the rest of the world.
2. Limitations on acceptable formats of X.509 certificates.
3. Special processing rules for X.509 certificates.
4. Extensions to X.509 PKI to allow delegation/impersonation of identities ('proxies').
5. Extensions to add group attribute information to proxies.

About 20 years later, the rest of the world has stuck with (1); items (2)-(5) have not been broadly adopted, leaving the technology burden – costs – with our community alone.

Migrating to Token-based credentials

Immense global efforts – governments and industries – have gone into securing the PKI technologies used on the Internet.

User credentials have largely not used X.509 technologies – but web-based global identity federations have been widely used and cemented.

One user credential technology is the JSON Web Token (JWT); widely used and becoming even more popular.

JWT is just a credential – it doesn't make for an AAI. **Like GSI**, we need to assemble other pieces.

- **Unlike GSI**, our community needs to invent fewer of the pieces.
- The key document is the WLCG Common Token Profile - https://zenodo.org/record/3460258 - which covers which RFCs utilized and the expected formats of the tokens where the RFCs are ambiguous.

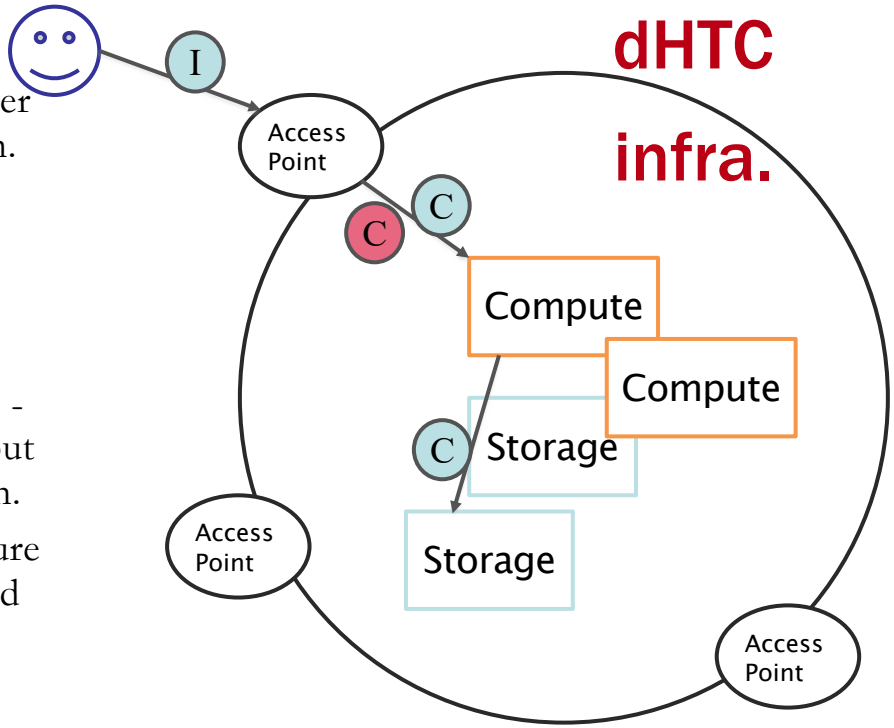
We are starting to see the first production use of the new AAI in time for Run3!

Leaving the identity behind

Tokens can be used for identity but their real power is they can make other statements of authorization.

- Tokens are issued by the experiment stating a particular action is permitted.
- This statement is honored by the resource provider.
- The identity may get logged for audit purposes - but the authorization is not from the identity but rather the embedded authorization in the token.

This moves the core of the distributed infrastructure to use **capability-based** authorizations as opposed to the **identity-based mapping**.



Outlook

- The WLCG common token profile was published in 2019.
- In 2020-2021, the various pre-existing prototypes were integrated together into a working infrastructure across OSG, EGI, and WLCG.
- In 2022, we're seeing first fruits – pilot jobs are being submitted with tokens this spring. OSG and HTHondor
- Big challenges remain:
  - Ensure token support in all our software, from ROOT on up.
  - Integrate and deploy token-based storage workflows into production use.
  - Tackle
- We will live in a hybrid model for awhile – with both infrastructures used.

MORGRIDGE
INSTITUTE FOR RESEARCH
RESEARCH COMPUTING

morgridge.org

This material is based upon work supported by the National Science Foundation under Grant No. 1836650. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

FEARLESS SCIENCE