OSG Software Bearer Token Transition Plan

Brian Lin
OSG Software Area Coordinator
University of Wisconsin–Madison

How did we get here?

- May 2017: Globus announces the Jan 2018 end-of-support for the open source Globus Toolkit (https://opensciencegrid.org/technology/policy/globus-toolkit/)
- Nov 2017: Grid Community Forum (https://gridcf.org/) is formed and begins supporting the Grid Community Toolkit (GCT) forked from the Globus Toolkit
- Dec 2019: OSG announces the next evolution of the OSG Software Stack (https://opensciencegrid.org/technology/policy/gridftp-gsi-migration/):
  - Bearer tokens for authentication and authorization
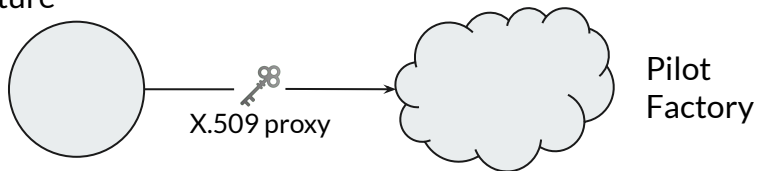 - HTTP/S for data transfer

What's next?

- Oct 2021 (WLCG milestone): pilot submissions may be performed with tokens
- Dec 2021 (WLCG milestone): WLCG VOMS admin servers retired in favor of IAM
- **Feb 2022: OSG 3.5 end-of-life.**
  - **GCT packages are no longer distributed in OSG Yum repositories**
  - **Remaining OSG packages have no GCT dependencies**
  - **XRootD supports X.509 and VOMS proxies without GCT dependencies**
- Mar 2022 (WLCG milestone): all storage endpoints on the WLCG provide support for tokens
- Mar 2023 (WLCG milestone): WLCG experiment data stageout and reads performed with tokens
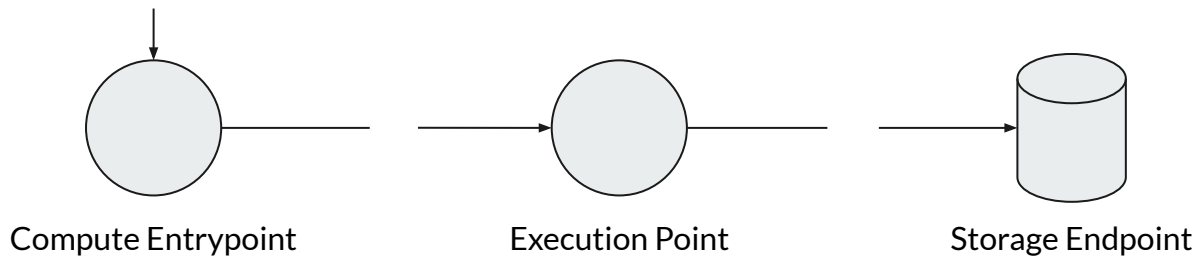- Mar 2024 (WLCG milestone): X.509 client authentication becomes optional

Authorization with X.509 proxies
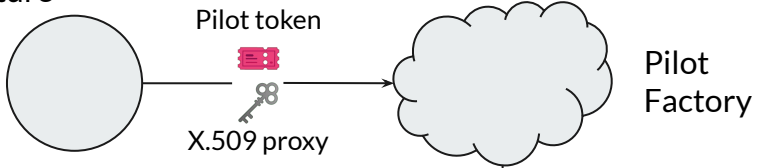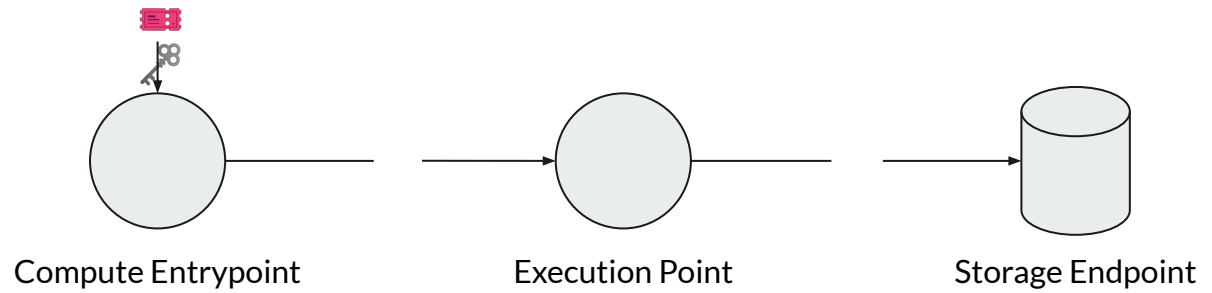
Collaboration
Infrastructure

X.509 proxy

Pilot
Factory

Collaboration/OSG

- -

Sites

Compute Entrypoint

Execution Point

Storage Endpoint

Pilot authorization with bearer tokens

Collaboration
Infrastructure

Pilot token

X.509 proxy

Pilot
Factory

Collaboration/OSG

Sites

Compute Entrypoint

Execution Point

Storage Endpoint

Full authorization with bearer tokens

Collaboration
Infrastructure

Pilot token

Storage token

Pilot
Factory

Collaboration/OSG

Sites

Compute Entrypoint

Execution Point

Storage Endpoint
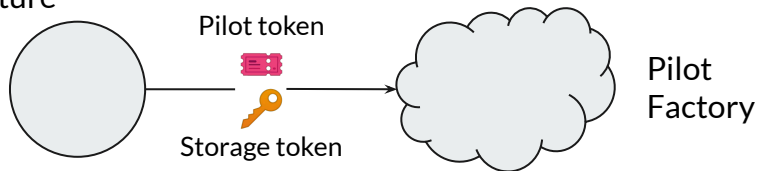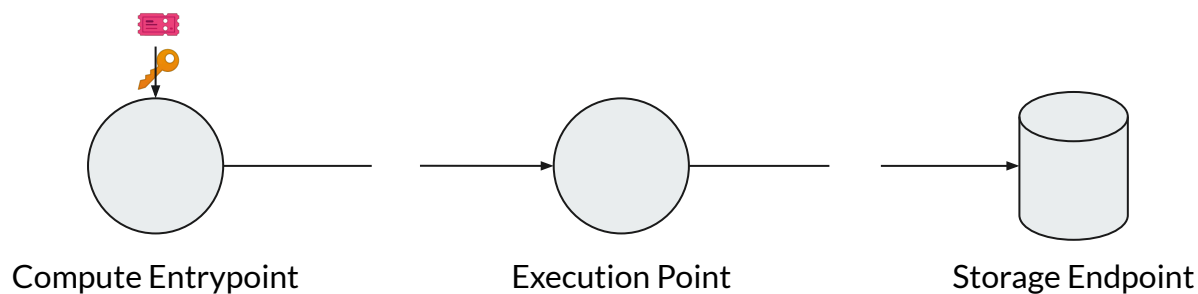
Attend tomorrow's Technical Working Sessions for more info about tokens!

11:00 CDT   Token AuthZ and Validation for Site Services (Derek Weitzel)
11:20 CDT   Bearer Token Hands-On (Derek)
13:00 CDT   HTCondor-CE Hackathon (Mátyás Selmeci)

Collaboration (VO) updates

- How to generate bearer tokens (from most feature-rich to least complicated)
  - Hashicorp Vault: supports OpenID Connect (OIDC) providers (e.g., CILogon, IAM), management of user and robot tokens, and integrates with HTCondor and Kerberos
    (See Dave Dykstra's European HTCondor Week talk
    https://indico.cern.ch/event/1059494/contributions/4532537/attachments/2312999/3938457/HTCondorEurope_Talk_Vault20210922.pdf)
  - If you only need robot tokens, use the `osg-token-renewer` service to keep your OIDC provider issued tokens up-to-date: https://opensciencegrid.org/docs/other/osg-token-renewer/
  - Alternatively, host a simple token issuer and make it available through OIDC Discovery over HTTPS
    - Renew your robot tokens regularly with the `scitokens-admin-create-token` command-line tool
    - For example, the OSPool uses files served over GitHub Pages: https://github.com/scitokens/osg-connect
- Plan pilot token → site user mappings:
  - Sites can map tokens to local users based on token issuer and subject
  - Evaluate whether or not your collaboration still needs multiple user mappings
- Provide the token issuer information and desired default user mappings to the OSG:
  help@opensciencegrid.org

Site updates: Compute Entrypoints

- Compute Entrypoints require HTCondor-CE 5 and HTCondor 9 (available in OSG 3.5 upcoming and OSG 3.6)
- If you have updated CEs, attend tomorrow's HTCondor-CE Hackathon to start receiving token-based pilots!
- **Recommended:** install from OSG 3.5 upcoming to support both token and X.509 based pilots https://opensciencegrid.org/docs/release/updating-to-osg-35/#updating-to-htcondor-ce-5
- If the collaborations you support are ready for token-only submission, install from OSG 3.6 https://opensciencegrid.org/docs/release/updating-to-osg-36/#updating-your-osg-compute-entrypoint

Site updates: Storage Endpoints

- Storage Endpoints require XRootD 5 (available in OSG 3.5 upcoming, expected in OSG 3.6 in ~2 weeks)
- OSG's XRootD standalone configuration provides external access to POSIX filesystems; supports HTTP-TPC; and accepts X.509 proxies, VOMS proxies, and bearer tokens: https://opensciencegrid.org/docs/data/xrootd/install-standalone/
- **Recommended:** wait ~2 weeks to install from OSG 3.6 when available as your configuration will need to change between OSG 3.5 and OSG 3.6
  - X.509 and VOMS proxy authentication is automatically handled by the default OSG configuration
  - Configure file access control using the XRootD auth file (updated documentation to come!)
- Install from OSG 3.5:
  - Configure X.509 and VOMS proxy authentication using LCMAPS https://opensciencegrid.org/docs/security/lcmaps-voms-authentication/
  - Configure file access control using the XRootD auth file https://opensciencegrid.org/docs/data/xrootd/xrootd-authorization/

Where to find us

- Join #software channel in the OSG Slack. Don't have an account? Request one at help@opensciencegrid.org
- Subscribe to the community mailing list, software-discuss@opensciencegrid.org: https://listserv.fnal.gov/scripts/wa.exe?SUBED1=SOFTWARE-DISCUSS&A=1
- Receive updates and release announcements: sites@opensciencegrid.org
- Found issues or need help? help@opensciencegrid.org

Questions?