Migrating to Token-based Authorization: Experiences & Lessons Learned

Jim Basney
jbasney@ncsa.Illinois.edu

HTC 23
Madison, Wisconsin
July 11, 2023

This material is based upon work supported by the National Science Foundation under Grant No. 2114989. 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.

Why?

- With the deprecation of GSI and proxy certificates, we have an opportunity to improve our authorization model
  - We don't want to simply reimplement GSI using JWTs
- Improve security using least privilege capabilities
- Improve usability and interoperability
  - Building on common JWT/OAuth technology
  - Coordinating across projects (LIGO, OSG, WLCG, etc.)
- Maintain the reliability and security of our cyberinfrastructure

- Our SciAuth project is focused on helping with this transition

https://sciauth.org/

How?

- Bi-weekly coordination meetings with WLCG, LIGO, Fermilab, etc.
- Hackathons & Interop Fests
- Phase in tokens while we phase out GSI proxy certificates
- Open Source SciTokens software
- Token issuers operated by CERN, CILogon, and OSG
- Using Hashicorp Vault for token management

How’s it going?

- In 2022, OSG successfully transitioned from proxy certificates to tokens via the OSG 3.6 release
- In February 2023, Fermilab began production with token-based authorization for their jobsub service. Now every payload job at Fermilab uses tokens.
- In May 2023, LIGO migrated core services to tokens for the start of the O4 observing run
- As of May 2023, both Virgo and LIGO have self hosted OSDF Origins providing SciTokens access to proprietary data via both OSDF and CVMFS
- WLCG token issuers in production at CERN for Alice, Atlas, CMS, and LHCb, on track to retire proxy certificates in WLCG by March 2026

Experiences & Lessons Learned

Balancing Scalability, Reliability, and Security

- Balance between shorter (security) and longer (scalability, reliability) token lifetimes
- Improvements to refresh token handling
  - Refresh token grace period at token issuers
  - Client acceptance of new refresh tokens (oidc-agent, vault, etc.)
- Timeouts and retries in token handling libraries (SciTokens)

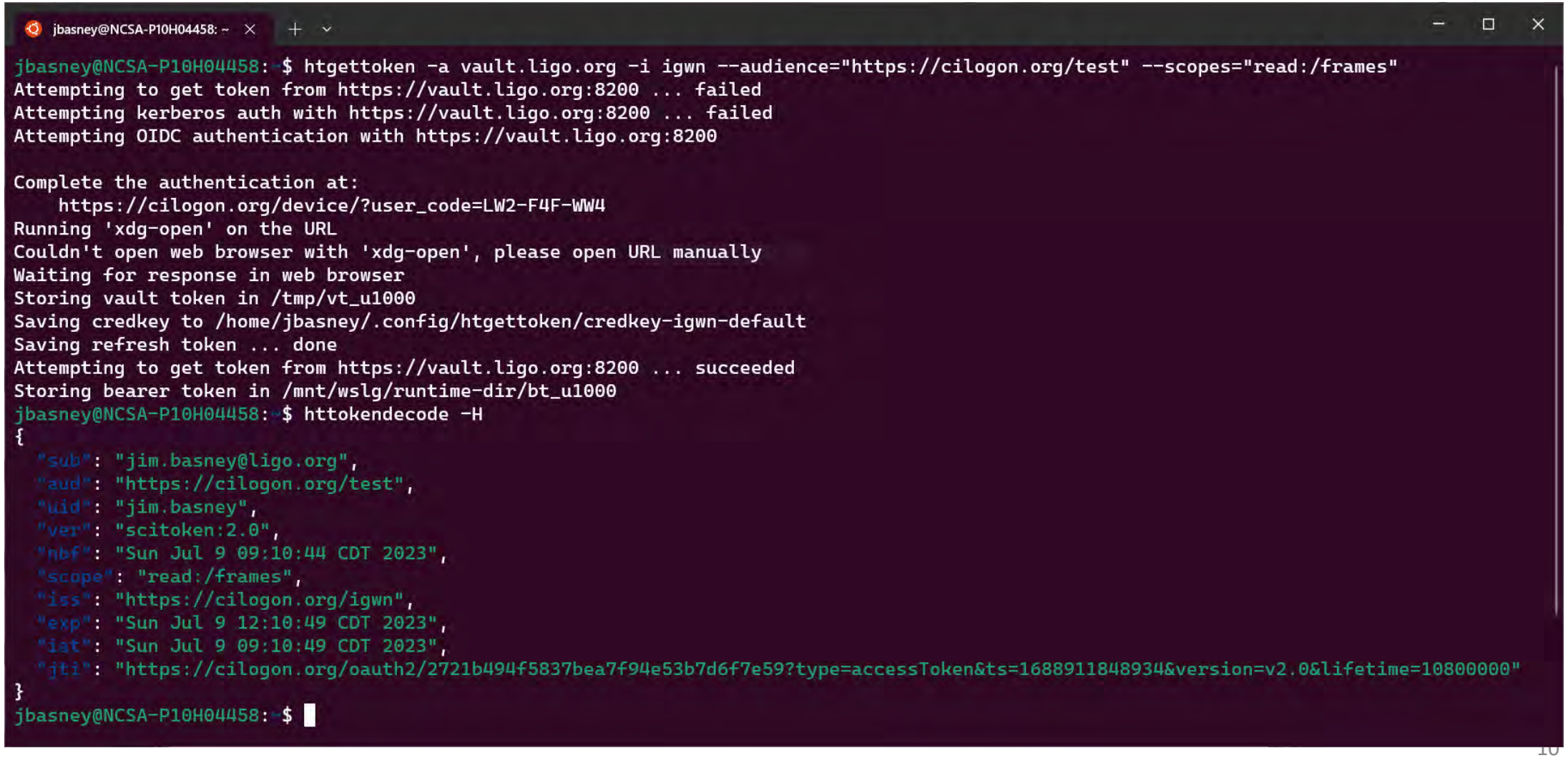
Authorization Policies

- Managing policies – revision control, LDAP
- Personal directories ("write:/staging/${uid}“)
- Robots
  - Access to “robot” tokens authorized via "Services:Robots:<robot-name>:SciTokens:authorized" groups

```
{
   "Issuers" : [
   {
      "IssuerName" : "IGWN",
      "Services" : [
         {
            "ServiceName" : "XRootD",
            "Scopes" : [
               {
                  "ScopeName" : "read:/frames",
                  "ScopeGroups": [
                     {
                        "EligibleGroup" : "cn=eligible_factor,ou=read-frames,ou=scopes,ou=SciTokens,ou=XRootD,ou=Services,ou=grouper,dc=ligo,dc=org",
                        "AuthorizedGroup" :"cn=authorized,ou=read-frames,ou=scopes,ou=SciTokens,ou=XRootD,ou=Services,ou=grouper,dc=ligo,dc=org",
                        "isMemberOf" : "Services:XRootD:SciTokens:scopes:read-frames:authorized",
                        "LDAP" : "ldaps://ldap.ligo.org"
                     },
                     {
                        "EligibleGroup" : "cn=CO:members:active,ou=groups,o=KAGRA-LIGO,o=CO,dc=gwastronomy-data,dc=cgca,dc=uwm,dc=edu",
                        "AuthorizedGroup" : "cn=CO:members:active,ou=groups,o=KAGRA-LIGO,o=CO,dc=gwastronomy-data,dc=cgca,dc=uwm,dc=edu",
                        "isMemberOf" : "gw-astronomy:KAGRA-LIGO:members",
                        "LDAP" : "ldaps://ldap.gw-astronomy.cilogon.org"
                     }
                  ]
               },
[…]
```

```
{
   "ScopeName" : "write:/staging/${uid}",
   "ScopeGroups" : [
      {
         "EligibleGroup" : "cn=LDGCITUsers,ou=CIT,ou=LDG,ou=LSC,ou=LVC,ou=Communities,ou=grouper,dc=ligo,dc=org",
         "AuthorizedGroup" :"cn=LDGCITUsers,ou=CIT,ou=LDG,ou=LSC,ou=LVC,ou=Communities,ou=grouper,dc=ligo,dc=org",
         "isMemberOf" : "Communities:LVC:LSC:LDG:CIT:LDGCITUsers",
         "LDAP" : "ldaps://ldap.ligo.org"
      },
      {
         "EligibleGroup" :
            "cn=CO:COU:LDG Grid Account Holders:members:active,ou=groups,o=KAGRA-LIGO,o=CO,dc=gwastronomy-data,dc=cgca,dc=uwm,dc=edu",
         "AuthorizedGroup" :
            "cn=CO:COU:LDG Grid Account Holders:members:active,ou=groups,o=KAGRA-LIGO,o=CO,dc=gwastronomy-data,dc=cgca,dc=uwm,dc=edu",
         "isMemberOf" : "CO:COU:LDG Grid Account Holders:members:active",
         "LDAP" : "ldaps://ldap.gw-astronomy.cilogon.org"
      }
   ]
}
```

Supporting Command-Line Interfaces



What’s next?

Migration Continues

- Completing phase-out of proxy certificates
  - CILogon plans to stop issuing X.509 certificates in 2025
  - WLCG on track to phase out certificates in 2026
- Further developing authorization policies
- Additional token integrations
  - CERN FTS – March 2024 WLCG data challenge
- Harmonizing SciTokens, WLCG, and EGI token profiles

What have we accomplished?

- Modernizing our authorization systems
- Improving our security posture
- A coordinated migration with minimal disruption

Thanks to the efforts of many people across many projects!

Thanks!

jbasney@ncsa.Illinois.edu

https://sciauth.org/