

Token-Based AuthN and AuthZ

Derek Simmel
FIM4R Meeting, CERN, Switzerland
February 15, 2023

Token-Based Authentication and Authorization

- Research computing infrastructures worldwide are working to migrate their legacy and X.509-based user authentication and authorization infrastructures to use OpenID Connect (OIDC, <https://openid.net/connect/>)
- OIDC is a protocol built on OAuth2 specifications that delivers identity and authentication information using JSON Web Tokens, (JWT, RFC 7519)
- OIDC is in widespread use in commercial web applications and services
- However, many research computing infrastructures have a significant investment in IAM protocols and services that are not (yet?) web-centric

Workshop Series 2020..2022

- WoTBAn&Az 2020: <https://indico.rnp.br/event/33/>
 - Token-based authorisation in WLCG, Globus Auth, LIGO's use of SciTokens, XSEDE's perspective on Token Assurance, Fermilab's transition to Token-based AAI
- WoTBAn&Az 2021: <https://sciauth.org/workshop/2021/>
 - Tokens in WLCG, Tokens in the TAPIS API Platform, Using CILogon OIDC Service for user authentication in Kubernetes, SciTokens at LIGO, HTCondor and OSG Token transition
- WoTBAn&Az 2022: <https://sciauth.org/workshop/2022/>
 - SSH with Federated Identities using OIDC, Token-based access to HPC resources in IRIS, Globus integration with NIH's Research Authentication Service and Common Fund Data Ecosystem, Adoption of SciTokens and WLCG Tokens by LIGO and Fermilab using CILogon

Token-Based AuthN & AuthZ @ TechEx

- *Moving to Tokens: IRIS & WLCG*, Tom Dack STFC
 - <https://sciauth.org/20221206-2-tdack-tokens.pdf>
- *CILogon and SciTokens*, Jim Basney, NCSA, Univ. of Illinois
 - <https://sciauth.org/20221206-3-jbasney-tokens.pdf>
- *Token-based AAI at Fermilab*, Jeny Teheran, Fermi Laboratory
 - <https://sciauth.org/20221206-4-jteheran-tokens.pdf>

SciAuth

- SciAuth is a U.S. National Science Foundation-funded project ([2114989](#)) that seeks to “improve the usability and interoperability of the security credentials that scientists use to access NSF cyberinfrastructure”
- <https://sciauth.org/>
- Co-sponsor of WoTBAn&Az workshops together with TAGPMA
- PEARC22 Paper: Brian Aydemir, Jim Basney, Brian Bockelman, Jeff Gaynor, Derek Weitzel (2022). *SciAuth: A Lightweight End-to-End Capability-Based Authorization Environment for Scientific Computing*
 - describes a containerized end-to-end environment for learning about and working with SciTokens
 - <https://dl.acm.org/doi/pdf/10.1145/3491418.3535160>

SSH Integration Examples

- pam-ssh-oidc + motley-cue, oidc-agent + ssh clients
 - as presented by Diana Gudu, Marcus Hardt, Gabriel Zachmann
Karlsruhe Institute of Technology
 - <https://github.com/EOSC-synergy/ssh-oidc>
- STFC PAM module
 - as presented by Jens Jensen et al, UKRI)
 - https://github.com/stfc/pam_oauth2_device