Authentication and Authorisation for Research and Collaboration

Tokens – Security Operations discussion

At CERN Security, Trust & Identity meetings – 5 Feb 2025

Hannah Short (CERN) & David Kelsey (STFC)
AARC-TREE and other projects

CERN, 5 February 2025

Tokens – Security Operations - Stakeholders

Federated Infrastructures & CSIRTs

- EGI, OSG, NeIC, EOSC, eduGAIN, WLCG, NGIs, …
- EGI CSIRT, CERN/WLCG, eduGAIN CSIRT, EOSC/EU Node…
  - Plus NREN CSIRTS, …..

Research Communities & Users

- VOs, Experiments, Users

Sites & Resource Centres

Other projects & working groups

- AARC-TREE, GN5-2 EnCo, AEGIS, FIM4R, WISE SCI-WG, ….
- WLCG AuthZ-WG, TTT-WG, WLCG Token TF
- EGI/WLCG Security Policy Group

AAI, IAM, AARC Proxies

- Operators
- Developers
- VO managers (AuthZ)

Tokens – Security Operations

- Traceability & Logging
  - Is it sufficient?
  - Configuration
- Software Vulnerability Handling
  - For Token and IAM technology
  - How much home-grown middleware?
- Policies
  - Which policies need changing?
  - New policies?
- Data protection and GDPR
- Emergency Suspension, Revocation
- Operational tools?
- Training
  - CSIRTs, IRTF, …
  - VO/Community security teams
  - EGI SVG
  - Do users need training?

Establishing Trust

- Risk Assessment
- Security Assessment
  - Architecture
  - Software
  - Deployent details
- AAOPS Guideline and maturity assessment
- How are components deployed and operated?
  - Workflows