Traceability and Central Suspension

Security Requirements

- Following many recent discussions
- One overriding security concern is traceability
  - Need to track activity in the context of an incident
  - Increasingly complex in the context of dynamic resources

Security Requirements

- Following many recent discussions
- One overriding security concern is traceability
  - Need to track activity in the context of an incident
  - Increasingly complex in the context of dynamic resources

- By extension: what capabilities for central suspension
  - do we have?
  - do we need?

Traceability status

- In current WLCG X.509 landscape, recent focus on split traceability:
  - With pilots, user information may be obscured
  - Partial information from site, partial information from VO security
  - This was conclusion of WLCG Traceability WG
- For tokens, what information, and where, can we extract user information?
  - Non-human-readable tokens
  - Who do security teams need to talk to to get this?
  - Sites … identity proxies…
  - How do we test/validate?

Central suspension

- What central suspension capability do we need to deploy
  - How do we technically deploy this?
- Where does this take place in a practical sense
  - Identity proxies
  - … ?
- A common approach here is optimal!
  - Are there ”quick wins” as part of a longer strategy?

Topics for consideration

- Tokens are **not** certificates
    - Shorter-lived
    - Already been discussing different token environment
        - Likely to evolve rapidly
- API for blocking could be useful
    - Develop based on experience?
    - Share with other communities?
- Central suspension = user not able to generate more access tokens

Outcomes of recent Authz meeting

- Keep it simple!
  - Will certainly evolve
- Tabletop exercise with operational security teams (EGI CSIRT+OSG)
  - Once workflow(s) are established
  - More regular instances of this as status evolves
- For suspension
  - Start with **process** not **technology**
  - For WLCG, 4 VO token issuers
    - Suspend at this level
  - For broader community
    - Again start with process: but don’t reinvent wheel
    - Standards-based approach a good one