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
  - Need to understand how this works regardless of way forward

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
  - Need to understand how this works regardless of way forward

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

Traceability (user activity)

- 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

- For tokens, what information, and where, can we extract user information?
  - Entirely opaque tokens
  - Who do security teams need to talk to to get this?
  - Sites/identity proxies…
  - How do we test?

Traceability (token issuer)

- From recent discussions, noted that depending on token issuer have different levels of issuer traceability in the tokens themselves

- What do we need
  - How do we extract this?

Central suspension

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

Next steps

- Gather thoughts from this meeting
- Discuss at next IAM Users Workshop
  - Summarise at GDB
- Identify who will take technical work forward
  - Who needs to give input