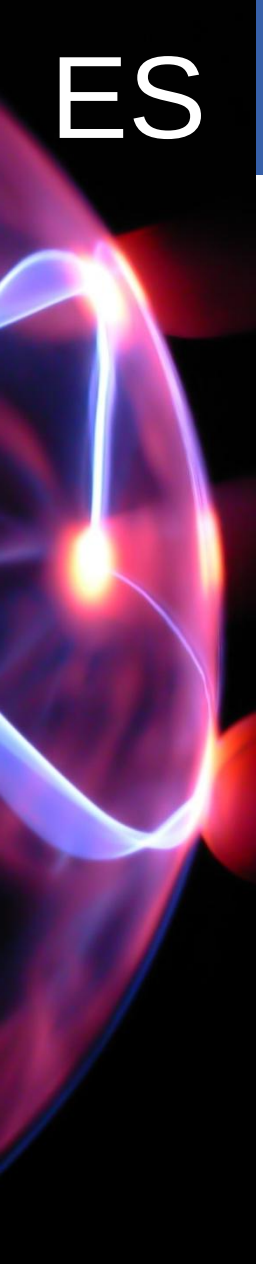

Security in data and storage management

Introduction & ideas

Maarten Litmaath

Performance

- X509 handshake is expensive
- What we can do now
  - Use bulk methods where possible
  - Use sessions where possible
  - Use trusted hosts where possible
    - ATLAS: PanDA VOBOXes trusted by LFC
- Should we look into short-lived cheap tokens?
- Consider a different model?
  - See next page

Security model

- X509 is the basis
  - Cannot change any time soon
  - 3 experiments base data access on X509 + VOMS
  - ALICE use it to bootstrap security envelopes
- Backdoors are to be closed !
- ALICE security envelopes
  - Specify pre-agreed access modes to pre-determined data
  - No need for general-purpose user proxies on WN
  - Might other experiments consider something similar at some point?

Typical/default X509+VOMS config

- Protect production data from users
  - ACLs and/or different mappings in SE
  - ACLs in catalog
  - Prevent tape access by users
- User data VO-readable and possibly VO-writable !
  - To be fixed where necessary

Desired X509+VOMS configuration

- Protect production data from users
  - ACLs and/or different mappings in SE
  - ACLs in catalog
  - Prevent tape access by users
- Analysis group data group-writable per group
- User data only accessible to the user
- Super users have access anywhere for their VO
  - Production managers? Separate VOMS roles?
  - Avoid bothering SE admin

- Which SE flavors support what? How easy?

Quotas

- Recent discussion in the weekly meetings suggests SE support for quotas is not really wanted any more
  - Quotas are handled centrally by the VO
  - Can we conclude this firmly?

- Else there would be some implications for security
  - Need for user and group quotas
  - Express them in terms of X509/VOMS?
  - API?