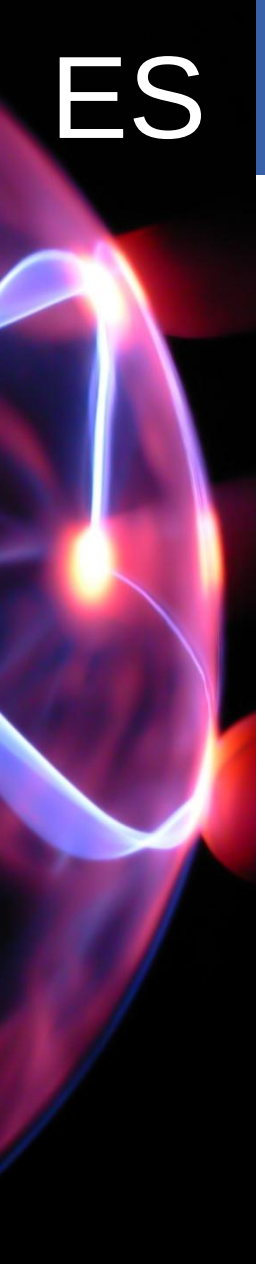


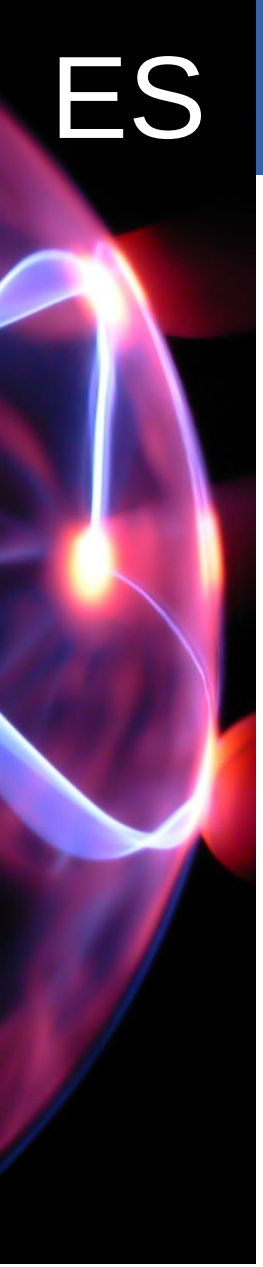
AAI usage, issues and wishes for WLCG

Maarten Litmaath
CERN

Outline

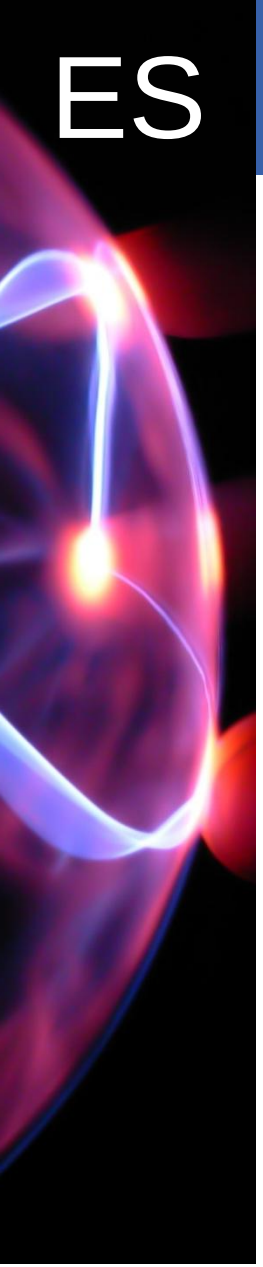
- Current AAI usage in WLCG
  - WLCG VOs: ALICE, ATLAS, CMS, LHCb
- Issues and wishes
- Conclusions

Current AAI usage (1)



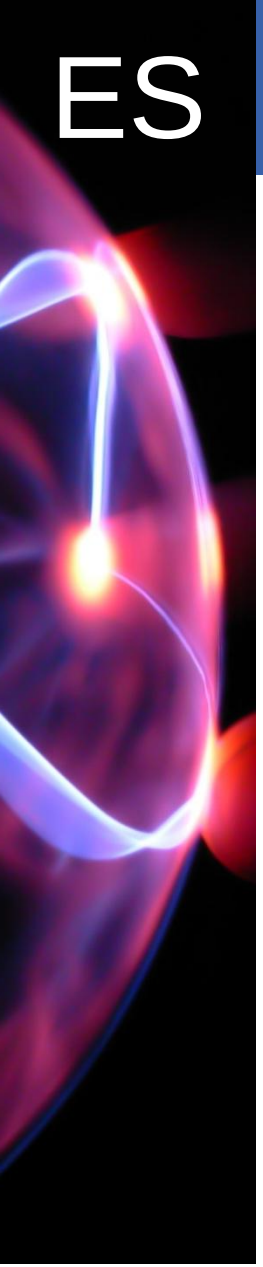
- X509 proxies with VOMS extensions
  - LHCb also include further extensions for their DIRAC data analysis services
- Certificates are obtained from national and HEP-specific CAs
  - Some institutes already use SLCS certificates linked to local or national identities
- A catch-all CA exists for LHC experiment members who do not have a national CA in IGTF yet

Current AAI usage (2)



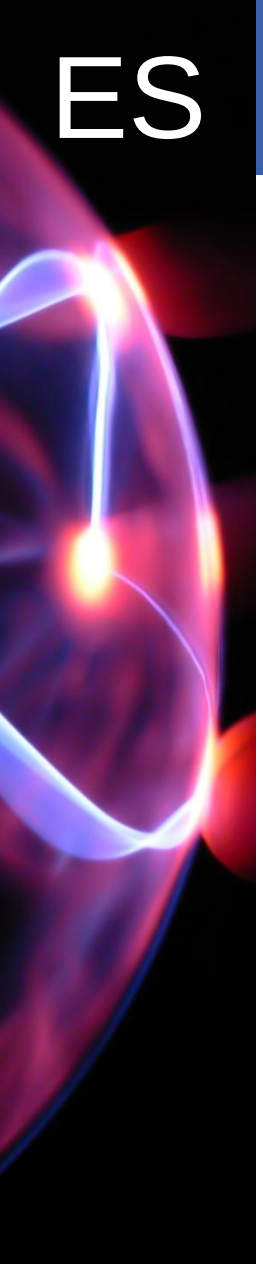
- A user is affiliated with an institute that participates in an LHC experiment
  - Vetting through CERN HR DB
- The user registers in the VOMS server of the experiment
  - Acquires attributes corresponding to the user's responsibilities
- The user can be suspended or removed from the VO by a VO admin
  - Hampered by use of multi-day VOMS proxies
  - Grid-mapfiles are updated every 6 hours

Current AAI usage (3)



- VOMS hierarchies of ATLAS and CMS have groups for various participating countries
  - Users can apply for membership of such groups
- A resource provider in such a country could give preferential treatment to affiliated users
  - When the country's group appears in the proxy
    - As primary FQAN
  - When the DN is recognized as a member of that group

Current AAI usage (4)

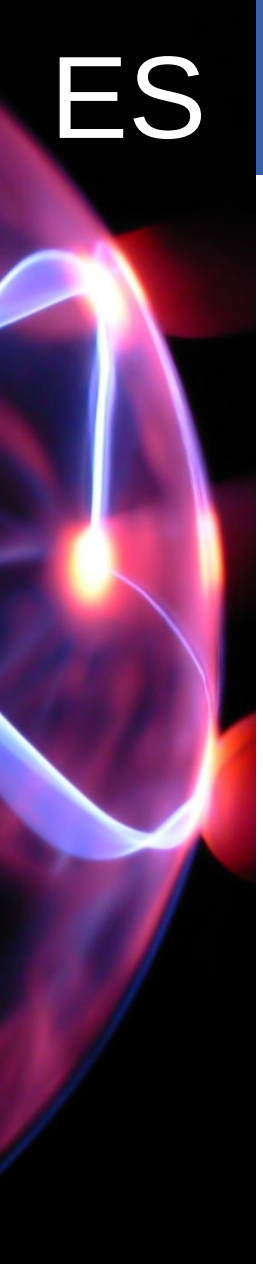


- Grid authorization methods
  - VOMS, grid-mapfile equivalents
- Resources accessed through the grid
  - Computing and storage elements
  - Catalogs, possibly other databases
  - Workload and data management services
  - Information, monitoring and messaging systems
    - BDII is world-readable
  - Proxy renewal services, VO agent nodes, …
    - MyProxy only requires trusted CA

Current AAI usage (5)

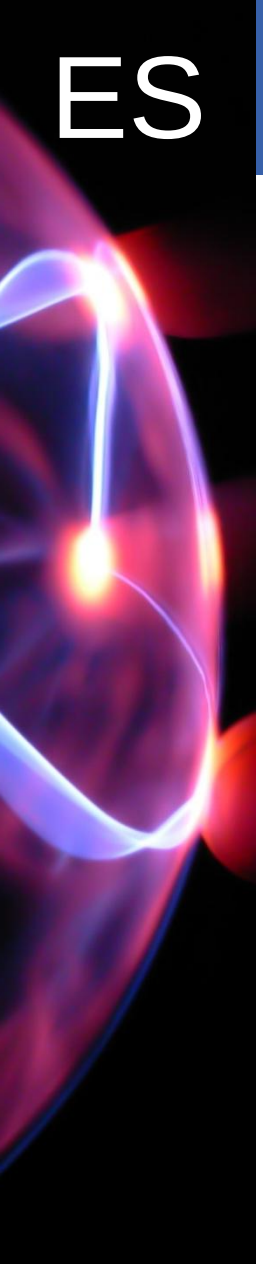
- Authorization for resources outside the grid
  - Local user or service account identity
- Resources accessed outside the grid
  - Computing and storage elements
    - Local batch submission
    - Local, possibly insecure “backdoor” data access
  - Catalogs, databases
    - DB account + password in configuration file
  - …

Current AAI usage (6)



- Authorization (if needed) for web resources
  - User certificate → grid-mapfile, or trusted CA
  - User name + password, or SSO
- Web resources
  - Catalogs, databases
  - Workload and data management portals
  - Information and monitoring systems
  - Operations, ticketing and accounting portals
  - Documentation, conferencing, …

Issues and wishes (1)



- VOMS lifetime may differ from proxy lifetime
  - VOMS renewal differs from proxy renewal
- Concurrent activities by the same user with different groups/roles can be tricky to manage
  - Beware not to use/overwrite the wrong proxy
  - “/tmp” is not shared across an interactive cluster

Issues and wishes (2)

- Conflicting uses of primary FQANs
  - To get the right treatment on the CE (queue/ priority/share) the primary FQAN is decisive
  - That FQAN may be undesirable for data operations
    - Need to grant artificial privileges for such FQANs in storage elements, catalogs, …
    - Regenerate proxy on WN for correct FQAN → fragile
  - Pilot systems may avoid such conflicts
  - Roles/groups could be associated with services
    - Each service applies what it recognizes

Issues and wishes (3)

- Web browsers cannot import VOMS proxies
  - Web services are limited to a grid-mapfile equivalent to regulate access
- Short-lived tokens should be used to access a service repeatedly → reduce AA overhead
- Standard OpenSSL/GSSAPI should be used instead of Globus
  - Avoid conflicting versions, reduce dependencies

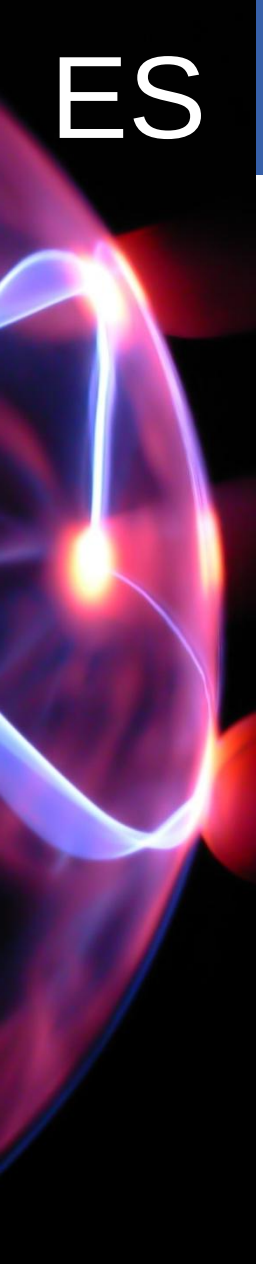
Issues and wishes (4)

- Users would like not to worry about proxy expiration
- Migration to a new certificate can be a hassle
  - Certificate validity could be increased to 3-5 years
    - People who left should be faster removed from their VO
  - DN change should be needed only exceptionally
- Proxy/token support at “OS” level might help
  - That looks far away

Issues and wishes (5)

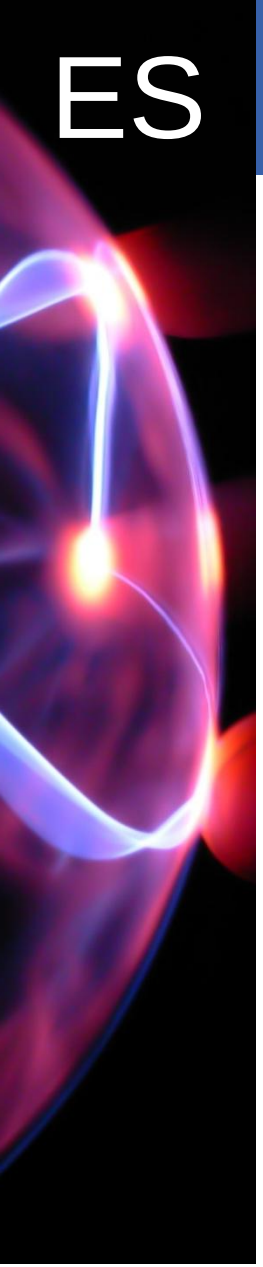
- Consistent implementation of shares and permissions across sites is difficult
  - Storage quotas essentially absent
  - VO super users desirable for data management
- Access rights synchronization across storage elements and catalogs is cumbersome
  - Consistency service demonstrator available for DPM and LFC

Issues and wishes (6)



- Service authorization ought to be improved
  - A valid host DN does not imply a valid service
  - Service certificates should be better supported
- Support for multi user pilot jobs should be simplified
  - The use of gLExec in setuid mode is cumbersome and fragile
  - This matter will be reassessed by the WLCG Technical Evolution Group on Security
    - Middleware wishes might come afterwards

Issues and wishes (7)



- Incoherence in service security models
  - Variety of libraries and configurations
  - Algorithm for deciding mapping or ACLs
    - VOMS, DN
  - Logging
    - Formats, contents
  - Banning
    - Impossible or awkward on some services
  - Testing/debugging/forensics tools
    - Available for some scenarios on some services
- There may be other issues not listed here

Conclusions

- The existing AAI schemes do allow the LHC experiments to use the WLCG infrastructure quite successfully
- Users and resource providers are not really satisfied with how grid security works today
- Various issues and wishes have been outlined on the preceding pages
  - Priorities to be assessed in the WLCG Technical Evolution Group on Security