Update on SHA-2 and RFC proxy support

Pre-GDB

2013-01-15

Maarten Litmaath

CERN

Update on the problem

- IGTF would like CAs to move from SHA-1 to SHA-2 signatures ASAP, to anticipate concerns about the long-term safety of the former
  - See https://twiki.grid.iu.edu/bin/view/Security/HashAlgorithms
- For WLCG this implied using RFC proxies instead of the Globus legacy proxies in use today
  - See Jan 2012 GDB presentation for detailed explanation
- On Dec 20 dCache project leader Patrick Fuhrmann wrote:
  - "We got the sha2 with jglobus to run with dCache."
- This means we "just" need to get SHA-2 working everywhere
  - Switch to RFC proxies later, at our convenience

Timelines

- SHA-2 certs to be issued not before Aug 1, 2013
- Aim to have the production infrastructure ready by that time
  - For EGI sites that goes with the end of EMI-1/UMD-1 support on Apr 30 plus a grace period of 3 months
    - Various components will only be OK in EMI-3/UMD-3
      - CREAM
      - dCache ?
      - StoRM
      - WMS
  - OSG will also phase out old versions by end of spring
- Monthly tracking of progress and blockers, if any
  - SHA-2 introduction date could be delayed further

Current state of affairs

- Various SW to be made ready for SHA-2
  - EMI/UMD/OSG components
  - Experiment-ware
  - Central EGI/OSG/WLCG services
- WLCG tracking page
  - https://twiki.cern.ch/twiki/bin/view/LCG/RFCproxySHA2support
- EGI Operations plans
  - Assess UMD components via SHA-2 test VO
  - Track production infrastructure uptake via SAM instance
    - VOMS servers for "ops" should support at least 1 SHA-2 CA
- SHA-2 CERN CA to become available this month
  - Alongside current CA
    - To be supported alongside IGTF CAs while not yet included, allowing for tests by experiments and "ops"
  - User and host DNs will not change

Updated phases and milestones

1. Deployment of SW supporting SHA-2 proxies
   - Proxy usage:
     - Legacy
     - SHA-2 → only in special tests
     - RFC → only in special tests
   - SW supports:
     - Legacy
     - SHA-2 → maybe
     - RFC → maybe
   - Milestone:
     - All deployed SW supports SHA-2 proxies → early summer?
   - Additional goal:
     - All deployed SW supports RFC proxies
       - Will come automatically in most cases
2. Introduce SHA-2 CAs → Sep?