Update on SHA-2 and RFC proxy support

GDB

2012-07-11

Maarten Litmaath

CERN

Reminder - 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 currently implies using RFC proxies instead of the Globus legacy proxies in use today
  - See Jan GDB presentation for detailed explanation
- Switching to using the EMI Common Authentication Library (CANL) may help here: supports SHA-2 with legacy proxies
  - Will be investigated by the dCache team
    - GSI based delegation not yet supported, should not be hard
  - Also BeStMan might use it then

IGTF plans

- EUGridPMA/IGTF discussed the matter at various meetings
  - https://www.eugridpma.org/meetings/2012-01/summary.txt
- Quote:
  - "The date by which SHA-2 production certs may be issued will be NO LATER than January 2013 (and it is likely we will RECOMMEND CAs to move then, since it will take another 395 days to get rid of SHA-1 in a reasonable way)"
- That would give us 5 months to get ready for RFC and SHA-2
  - Looks impossible, in particular now that this year's LHC run will be extended a few months into 2013 !
    - Neither experiments nor sites will want to rock the boat ...
- A Plan B would be desirable → read on ...

Current state of affairs

- There are various pieces of middleware and experiment-ware that need to be made ready for SHA-2 or RFC proxy support
  - SHA-2: dCache, BeStMan (RFC proxies already supported by these)
  - RFC: Argus, CREAM, WMS, DIRAC, ...
  - Central EGI/OSG/... services
  - https://twiki.cern.ch/twiki/bin/view/LCG/RFCproxySHA2support
    - EGI Operations will help with the assessment
- All EMI-2 products (released May 21) should support RFC proxies
  - WMS not yet available
  - Very little uptake so far
  - Also SHA-2 should be supported, except for dCache – verified?
- It may be many weeks before the affected products can be endorsed by UMD for generic deployment on EGI sites
  - EMI-2 is a major release with many changes
- OSG did not report additional constraints for their MW

Updated phases and milestones (1)

1. Deployment of SW supporting RFC proxies
   - Proxy usage:
     - Legacy
     - RFC → only in special tests
     - SHA-2 → only in special tests
   - SW supports:
     - Legacy
     - RFC → maybe
     - SHA-2 → maybe
   - Milestone:
     - All deployed SW supports RFC proxies → summer 2013 ?
   - Additional goal:
     - All deployed SW supports SHA-2, except dCache and BeStMan → summer 2013 ?

Updated phases and milestones (2)

2. Switch to RFC proxies → summer 2013 ?

3. Upgrade dCache and BeStMan
   - Proxy usage:
     - RFC
     - SHA-2 → only in special tests
   - SW supports:
     - RFC
     - SHA-2 → maybe
   - Milestone:
     - All deployed SW supports SHA-2 → autumn 2013 ?

4. Introduce SHA-2 CAs → Jan 2014 ?
   - Plan B ?!

Plan B proposal

- Introduce a new, short-lived WLCG catch-all CA
  - It would issue SHA-1 certificates to any WLCG member whose CA no longer supports SHA-1 for new certificates
    - Name space "*"
    - Users
    - Hosts, services
  - Its own cert would be distributed in addition to the IGTF CAs
    - As used to be done for the FNAL KCA
  - Its lifetime would be 1 or 2 years, just to bridge the gap
  - It would need to be in place before Jan 2013
    - Unless IGTF shift their timeline
  - A significant effort ...
- Our RFC and SHA-2 conversion efforts continue in parallel