Update on SHA-2 and RFC proxy support

GDB

2012-04-18

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 implies using RFC proxies instead of the Globus legacy proxies in use today
  - See Jan GDB presentation for detailed explanation

IGTF plans (1)

- The EUGridPMA discussed the matter at their Jan meeting
  - 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 8 months to get ready for RFC and SHA-2
  - Looks rather tight/optimistic
    - Details on the following pages
- A Plan B would be desirable → read on …

IGTF plans (2)

- On March 14 a (closed) SHA-1 discussion list was created
  - WLCG is well represented
- Goal is to assess the risks of various SHA-1 attack scenarios
  - Define mitigations where possible
  - WLCG use cases need not always be concerned
- This may buy us extra time in the end
  - We still need to pursue our RFC + SHA-2 preparations!
- IGTF May 7-9 meeting at KIT will have F2F discussion

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, …
    - SHA-2 should work, not tested…
      - VOMS needed a bugfix!
- A TWiki page will detail the state of affairs
- For EMI products the current time line is the EMI-2 release in April/May
  - OSG are also aware and did not report additional constraints
- 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

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 → late autumn 2012 ?
   - Additional goal:
     - All deployed SW supports SHA-2, except dCache and BeStMan → late autumn 2012 ?

Phases and milestones (2)

2. Switch to RFC proxies → Jan 2013 ?
   - There should be no issues with that by this time
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 → by spring 2013 ?
4. Introduce SHA-2 CAs
   - Plan B ?!