Update on SHA-2 and RFC proxy support

GDB
2012-09-12
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 update

• EUGridPMA/IGTF further discussed the matter 2 days ago in their meeting at IN2P3-CC
  – http://agenda.nikhef.nl/conferenceDisplay.py?confId=2083
  – WLCG represented by Dave Kelsey and Maarten
  – Minutes are attached to the agenda page

• Current thinking about time lines:
  – 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
  – Monthly tracking of progress and blockers, if any
    • SHA-2 introduction date to be delayed further as needed
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](https://twiki.cern.ch/twiki/bin/view/LCG/RFCproxySHA2support)
    • EGI Operations will help with the assessment

• All EMI-2/UMD-2 products should support RFC proxies
  – WMS not yet available
  – Little uptake so far
    • Bugs were found and fixed, workarounds provided \(\rightarrow\) can go faster now
  – Also SHA-2 should be supported, except for dCache \(\rightarrow\) verified?

• OSG did not report additional constraints for their MW
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 → spring 2013 ?
   – Additional goal:
     • All deployed SW supports SHA-2, except dCache and BeStMan → spring 2013 ?
Updated phases and milestones (2)

2. Switch to RFC proxies → spring 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 → summer 2013?

4. Introduce SHA-2 CAs → autumn 2013?