SHA-2 and RFC proxy support

GDB

2012-01-11 + updates

Maarten Litmaath

CERN

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

- dCache and BeStMan use JGlobus 1.x, which does not support SHA-2
  - Not easy to add
  - That (dead) code also has performance issues

- JGlobus 2.x does support SHA-2, but appears to support only RFC proxies and _not_ the Globus legacy proxies being used today
  - Legacy support would not be easy to add
  - Who might actually do it ?

- JGlobus 2.x also cannot handle CAs that still have the emailAddress attribute in their DN or signing policies
  - WLCG currently relies on 3 such CAs with ~130 users in total

Current state of affairs and ideas

- 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…
- For EMI products the current time line is the EMI-2 release in April/May
  - OSG ?
- It may be many weeks before the affected products can be endorsed by UMD for generic deployment on EGI sites → run into the summer holidays
  - EMI-2 is a major release with many changes
- During the whole time the LHC run will be ongoing and nobody will be keen on significant upgrades → rather target December
- Nobody wants to upgrade right before the Xmas period, so we end up in early 2013, right after the winter conferences…
- We would have a year to get the 3 CAs fixed
  - Affected users could also use their CERN CA certificates instead
  - Affected services would not have an obvious alternative

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
   - Additional goal:
     - All deployed SW supports SHA-2, except dCache and BeStMan

Phases and milestones (2)

2. Switch to RFC proxies and 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

3. Introduce SHA-2 CAs