CERN CA: SHA-2 and Code Signing Certificates

Paolo Tedesco
CERN - IT/OIS

26th EUGridPMA and IGTF All Hands meeting, Lyon

12/9/2012

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

Agenda

- SHA-2 support
  - Goals
  - Implementation plan
- Code signing certificates

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

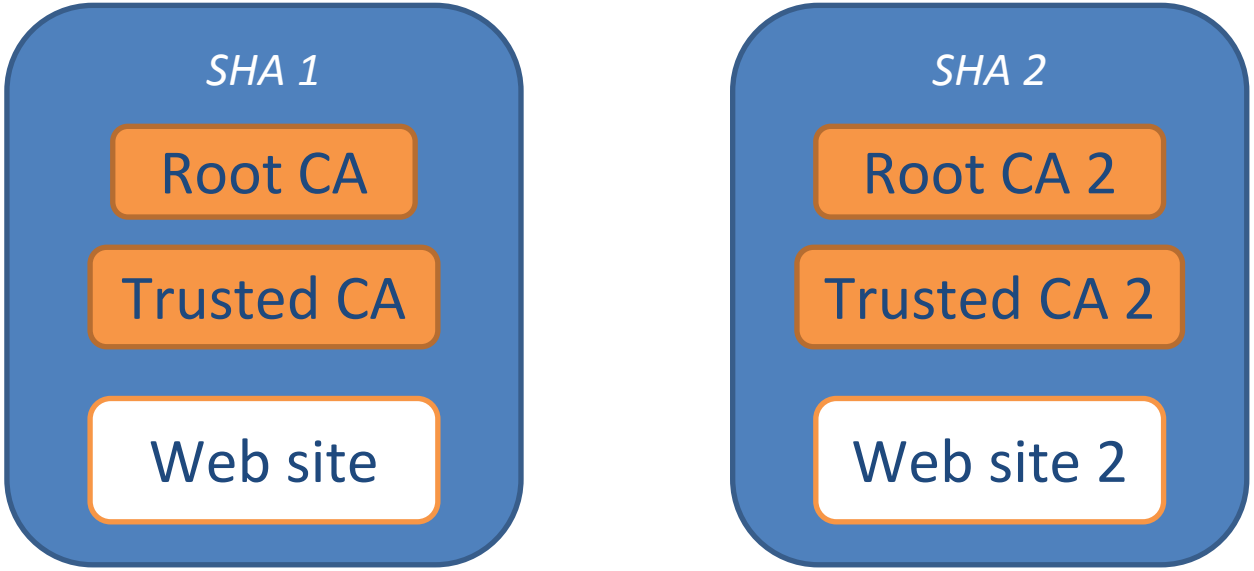
SHA-2 support: goals

- Don’t modify existing infrastructure
- Provide SHA-2 on-demand
- Allow middleware testing
- When everything ok => make default

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

SHA-2 support: plan

- Duplicate the existing hierarchy
- Exactly same settings and policies
- Ideally:
  - Enforce minimum key length = 2048
  - Increase Root & Trusted key length = 4096



CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

SHA-2 CA Accreditation

- Based on currently approved CP/CPS
  - Exactly the same with new OIDs
- Nothing new to negotiate
- Ideally a simple offline review

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

Code Signing Certificates

- Currently not supported
- Robot certificate with extra bit
  - Issued following robot certificate policies
  - 2 years validity
- Issued to users at CERN
- Requests handled by web site

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

- Questions?

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it