The CERN CA SHA-2 Infrastructure

Paolo Tedesco
CERN - IT/OIS

29th EUGridPMA meeting

Bucharest 9/9/2013

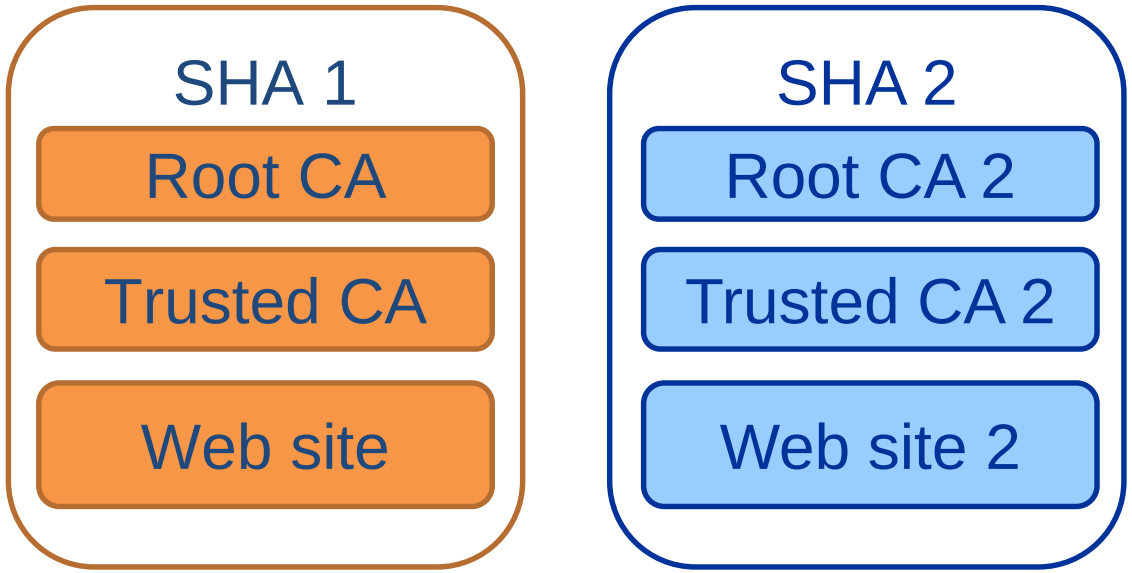
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

Overview

- SHA-2 CA at CERN
- Improvements
- Timeline

CERN's SHA-2 plan

- Presented and approved in Lyon (Sep. 2012)
- Duplicate the existing hierarchy
  - Same settings and policies (with new OIDs)
- Microsoft PKI implementation
  - Easier to support



Hierarchy

SHA-1 Infrastructure

CERN Root CA

CERN Trusted Certification Authority

http://cern.ch/ca
Grid user
Grid user on Smartcard
Grid host
Grid robot
Domain Controller

SHA-2 Infrastructure

CERN Root Certification Authority 2

CERN Grid Certification Authority

OCSP

CERN Certification Authority

http://cern.ch/gridca
Grid user
Grid host
Grid robot

http://cern.ch/cernca
Code Signing

CERN only

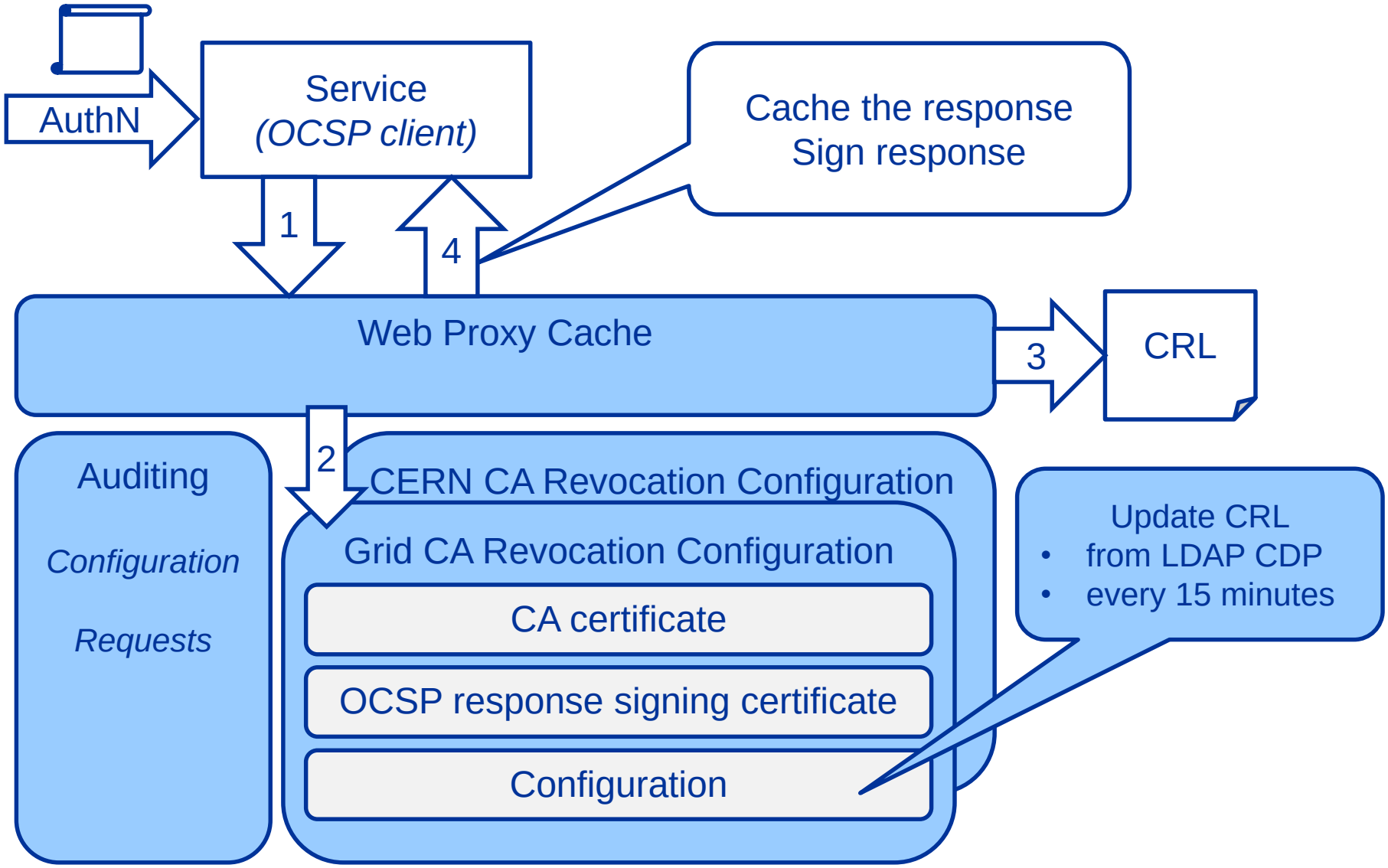
http://cern.ch/cafiles
CA certificates
CRLs
CP/CPS docs

The CERN CA SHA-2 Infrastructure

Improvements

- SHA-2 (sha512) used as a hash algorithm
- Increased key lengths
  - Root and intermediate CAs: 2048 -> 4096
  - Minimum required for certs: 1024 -> 2048
- Static files in separate web site
  - Cleaner deployment processes
  - Scale (load-balance) sites independently
- Non-GRID certificates moved to “internal” CA
  - Code Signing
- Online Certificate Status Protocol (OCSP) service

Microsoft's OCSP



Deployment and scaling

Offline root CA
CERN Root Certification Authority 2

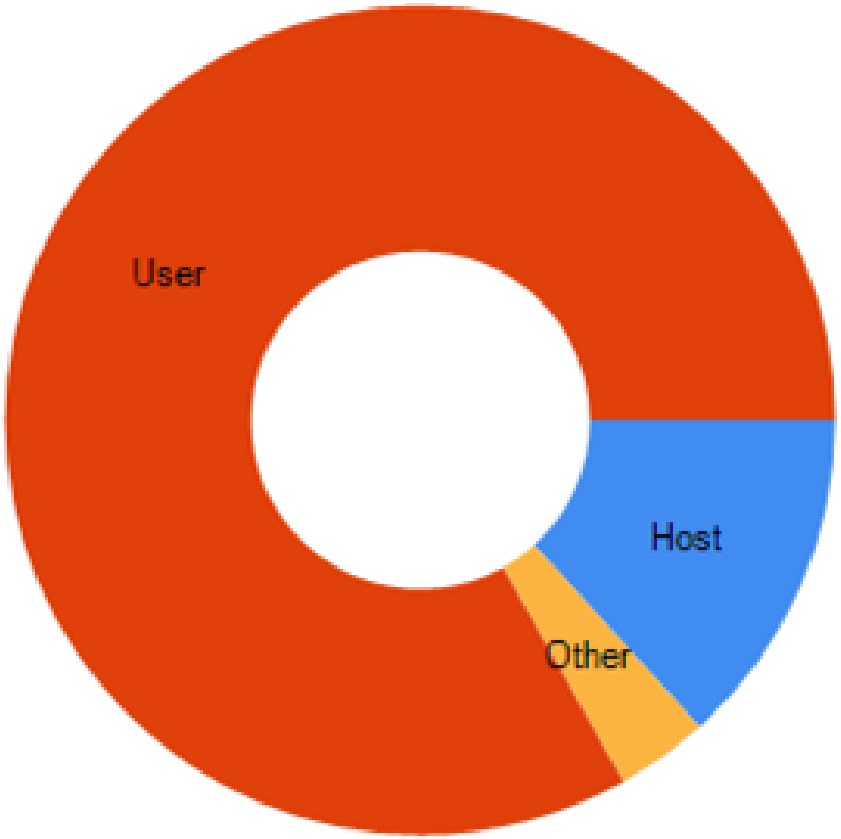
Online issuing CA (with HSM)
CERN Grid Certification Authority

Frontend website
http://cern.ch/gridca
http://cern.ch/cafiles
http://ocsp.cern.ch/ocsp

- Can add issuing CAs
  - Requests volume
  - Compromised CA
- Scale web sites
  - CRL distribution
- OCSP array configuration
- Most likely not necessary

Issued certificates

Certificates by type (Today)



Name	Color	Total
Host		11
Other		3
User		69

Timeline

EUGridPMA

Now

CERN

- Should use SHA-1
- Can use SHA-2

- Grid CA as pilot

1st October 2013

- Begin SHA-1 phase out
- SHA-2 as default

- Reduce certificates validity to 180 days

1st June 2014

- Stop issuing SHA-1 certificates

1st December 2014

- SHA-1 certificates expired / revoked

1st January 2015

- Start SHA-1 CA decommissioning

Conclusion

- SHA-2 CA at CERN is ready
- Same policies
- Improvements in the infrastructure
- Providing an OCSP
- Can proceed to SHA-1 decommissioning
  - According to last agreed timeline (to review?)