SHA-1 CAs in WLCG

WLCG Ops Coordination meeting

Nov 6, 2025

M. Litmaath

v1.0

The problem

- Some CAs still make use of SHA-1 in their root certificates and/or CRLs
  - More details on the next pages

- As of EL9, support of SHA-1 is by default disabled by the OS
  - For OpenSSL as well as Java

- On EL9, the minimal way to re-enable SHA-1 is to run the following command on the relevant hosts and reboot them
  - *update-crypto-policies --set DEFAULT:SHA1*

- On EL10, the only standard recourse is to re-enable **all** legacy algorithms
  - *update-crypto-policies --set LEGACY*
  - One could add a SHA-1 policy the way it is done on EL9 and enable just that

- Site admins do not like to re-enable **any** legacy algorithms!
  - Sooner or later, some may even be forbidden to do so!

CAs using SHA-1 in some way(s)

- The list is maintained here

- Root certificates
  - ASGCCA-2007
  - ArmeSFo
  - CESNET-CA-Root
    - **Superseded** by CESNET-CA-5
  - DFN-GridGermany-Root
  - DZeScience
  - DigiCertAssuredIDRootCA-Root
  - DigiCertGridRootCA-Root
  - IHEP-2013
  - KEK
    - **Superseded** by KEK2024
  - RomanianGRID
  - SRCE
  - SiGNET-CA
  - seegrid-ca-2013

- CRLs
  - ArmeSFo
  - DigiCertGridRootCA-Root
  - IHEP-2013
  - PK-Grid-2007
  - RomanianGRID

- DigiCert is leaving IGTF

How does that matter?

- The installed CA root certificates are trusted by construction: why should their signature algorithms be checked at all?

- Good news: most of our SW actually does **not** do that!
  - OpenSSL does not do that by default (which is how we use it)
  - Java → checked for dCache by Petr Vokac
  - dCache relies on **canl-java** for certificate validation, like StoRM
  - The canl-java developer (now: maintainer) confirmed that behavior

- Exception:
  - **XRootD < 5.7.0**
    - And no way to change the behavior in affected versions

- CRLs are a different story!
  - If SHA-1 is not enabled, **fetch-crl** will reject SHA-1 CRLs
  - OpenSSL is fine with CRLs being absent
  - For services based on canl-java this depends on its configuration → to be checked
  - Services may work with absent CRLs, but some security functionality would be lost

What shall we do about this?

- As a minimum, all relevant **CRLs** should switch to SHA-2 **ASAP**
  - That should be a lot easier than setting up a new CA
  - Recently, an affected CA fixed its CRL in just 1 day!

- While it appears that today, root certificate signature algorithms are not checked by recent MW versions, this might not remain so
  - Our situation may again be forced by external entities or circumstances
  - And many XRootD services still need to be upgraded

- Therefore a **deadline** is proposed for SHA-1 support in WLCG: **the end of 2026**
  - That would give all relevant CAs a full year to set up a new CA or have their customers switch to an alternative CA (e.g. GEANT TCS)

- Discussion…