New Grid Canada CA Proposal

Lixin Liu
Simon Fraser University

Grid Canada History

- Previously managed by NRC/CANARIE/SSC
- First version of Grid Canada CA was in production around 2003, mostly at request of WestGrid to use gridftp services and for Atlas researchers
- ‘New’ CA was rebuilt around 2010 using OpenCA
- SFU took over the ownership on April 1, 2016
- Offline signing only
- No. of certificates: 2500 users and 200 hosts/services
- Supported request methods: SSCEP and HTTPS
- Root CA expires in 2026
- Both OS and software require upgrade/rebuild

User Community

- HEP experiments
  - Atlas LHC, 1 T1, 4 T2 and some T3 sites
  - SNO+
  - Icecube
  - T2K
  - LIGO
  - Bell II
- WestGrid GridFTP and SSH services (retired now)
- Compute Canada Globus endpoints
- SKA

Physical Security

- SFU data centre is located in the basement of Water Tower Building (WTB)
- Access to WTB is restricted to selected number of SFU IT staffs only. Visitors must be accompanied by authorized IT members.
- Operators on duty 7/24
- All access to DC is recorded
- Higher restriction for locked cage is available in with biometric reader. Facility is RCMP certified

New Grid Canada CA

- Self signed Root CA to be located inside locked cage
- Root CA uses OpenSSL to issue an Online CA certificate
- Root CA DN

  /DC=ca/DC=gridcanada/CN=Grid Canada Root CA
- Online CA will be located in locked rack with public network connection
- PKI software choice: EJBCA or OpenXPKI
- Plan to purchase HSM for Online CA
- Online CA DN

  /DC=ca/DC=gridcanada/CN=Grid Canada Online CA

Certificate Extensions

- Current CP OID is from NRC, Canada

  Policy: 2.16.124.101.1.274.47.1.1
- New CA uses SFU OID (SFU.RCG.GC.CP.CA)

  Root CA Policy: 1.3.6.1.4.1.325.10.1.1.1.<ver>

  Online CA Policy: 1.3.6.1.4.1.325.10.1.1.2.<ver>
- Classic X.509 CAs with secured infrastructure

  Policy: 1.2.840.113612.5.2.2.1

Certificate Subjects

- New subject prefix: /DC=ca/DC=gridcanada
- User certificates (OU is optional)

  /O=<institution>[/OU=People]/CN=<full name>/CN=<identity>
- Host and service certificates (both O and OU are optional)

  /[O=<institution>/][OU=host/]CN=<server FQDN>

  /[O=<institution>/][OU=service/]CN=<service>/<server FQDN>
- All certificates have subjectAltName email
- Host certificates should have one or more SAN dns
- Identity is CCI or institutional employee/student ID

/DC=ca/DC=gridcanada/O=computecanada.ca/CN=Lixin Liu/CN=bdw-000

/DC=ca/DC=gridcanada/CN=ldap/cedar.computecanada.ca

Identity Vetting

- Each Compute Canada user has an unique CCI and they are verified by both sponsors (PIs) and Compute Canada staff members at the local institution
- Compute Canada users should use CCI to enroll
- Only members from Canadian public institutions and government research labs are accepted
- Host and service certificate requests can only come from Compute Canada staff members
- All requests will be verified by Grid Canada staffs

compute canada | calcul canada

Questions, Suggestions?

- Root CA CRL lifetime, 1 years?
- Does the Root CA (offline only) require a HSM?
- Both Root and Online CA are running in VMs so they can be moved to new hardware when necessary
- Encrypted filesystem for VMs?
- HSM options (talking to nShield and SafeNet)?
- Self-encrypted USB drive to store VM/private keys?

  Apricorn Aegis Secure Key 3Z 16GB

https://www.amazon.ca/Apricorn-Hardware-Encrypted-Validated-ASK3Z-16GB/dp/B01N4U7GNA