KISTI Grid CA

Korea Institute of Science and Technology Information
Supercomputing Center
Jae-Hyuck Kwak(jhkwak@kisti.re.kr)

APGrid PMA VTC meeting(2005-07-26)

Introduction

- KISTI Grid CA has been operating by Korea Institute of Science and Technology Information(KISTI) in Daejeon, since April 2002
- KISTI Grid CA provides X.509 certificate for K*Grid project and National e-Science project in Korea

History

- KISTI has been operating an experimental-level CA from April 2002 for the K*Grid project and the other Grid community in Korea
- KISTI Grid CA has approved as a production-level CA by APGrid PMA from August 2004
- KISTI Grid CA has included in KMI-R1 package as K*Grid CA
  - ▶Provide web-based interface
  - ▶Download it from http://www.moredream.org
  - ▶Everyone can construct their own Grid CA service as the alternative of Simple CA
- http://ca.gridcenter.or.kr

CP/CPS

- CP/CPS version 1.3 from August 9, 2004
- Download it from https://ca.gridcenter.or.kr/CPS/KISTI-GRID-CA-CP-CPS-V1.3.pdf
- Object ID is 1.3.6.1.4.1.14305.1.1.1.1.3

End Entity

- Person, computer, and service
  - ▶ Korean domestic individuals participating in K*Grid project and National e-Science project
- Certificate type
  - ▶ User certificate
    - /C=KR/O=KISTI/OU=XXX/CN=XXX
  - ▶ Host certificate
    - /C=KR/O=KISTI/CN=host/XXX
  - ▶ Service certificate(LDAP)
    - /C=KR/O=KISTI/CN=ldap/XXX

Identification and Authentication

- A certificate requester must have a login account for the KISTI Grid CA web site
- To register to KISTI Grid CA web site, a user should contact to the CA admin and provide some personal information (name, e-mail, organization)
- The CA admin contact to the user by phone or face-to-face meeting
  - ▶Currenty, KISTI Grid CA is used only by the participants of K*Grid project and National e-Science project
- A certificate requester can request either user certificate or host/service certificate through the web site

Certificate Restriction

- Certificate Lifetime for
  - ▶KISTI Grid CA root certificate is 5 years
  - ▶End entity is 1 year
- User certificate should not be shared

Certificate Revocation

- A certificate requester can request the revocation for his/her certificate, which is revoked by the admin
- CRL is updated immediately after every revocation, and reissued 7 days before expiration even if there have been no revocations
- The lifetime of the CRL is 30 days

Physical Security

- The CA signing machine is
  - ▶A dedicated machine
  - ▶Not connected to any network
  - ▶Locate in a separated room restricted to authorized personnel
    - Currently, not in a dedicated room, but in a testbed operation room
  - ▶Have CA private key and pass phrase stored in USB flash memory

Records Archival

- The following events are recorded and archived
  - ▶Certificate requests
  - ▶Issued certificates
  - ▶Revocation requests
  - ▶Issued CRLs
  - ▶All email messages send to ca@gridcenter.or.kr
  - ▶All email messages send by ca@gridcenter.or.kr
- All certificate requests and confirmations are logged in the database
- The minimum retention period is 3 years

Key Pair

- End entities' cryptographic keys are locally generated by their application during the requesting process
- KISTI Grid PKI doesn't generate private keys for user/host/service certificate and has no access to the end entities' private key
- Key size
    - ▶ The minimum key length for user/host/service certificate is 1024 bits
    - ▶ The root CA key length is 2048 bits

Future Plan

- For more security of KISTI Grid CA, we have a plan to enable HSM by the end of this year or the early of the next year
- For more reliable operation of KISTI Grid CA, we have a plan to cooperate with National S&T Information Security Center

Contact Information

Jae-Hyuck Kwak
Grid Technology Research Department, KISTI
305-806 Eoeun-dong 52, Yusung-gu, Daejeon, Korea
Phone: +82-42-869-0649
Fax: +82-42-869-0599
Email: jhkwak@kisti.re.kr

Sangwan Kim
Grid Technology Research Department, KISTI
305-806 Eoeun-dong 52, Yusung-gu, Daejeon, Korea
Phone: +82-42-869-0568
Fax: +82-42-869-0599
Email: sangwan@kisti.re.kr

감사합니다

Thank you

Danke

Merci

谢谢

ありがとう