NCHC CA

Alex Wu

January 17, 2006

Introduction

- NCHC:

  National Center for High-performance Computing.

- NCHC CA: issued and managed by NCHC, Taiwan.

CP / CPS

- Current version: 1.1.0 (November, 2005).
- Object ID:1.3.6.1.4.1.23308.1.1.1.0
- Based on RFC 2527.
- Managed by NCHC PMA: Any change in CP/CPS needs to be approved by the NCHC PMA.

End Entity

- Users of National Center for High-performance Computing (NCHC).
- Users of National Applied Research Laboratories (NARL).
- Users or services involved in KING (Knowledge Innovation National Grid) and TWAREN (TaiWan Advanced Research and Education Network) Projects.
- Users or services, such as government organizations, academic communities, and hospitals, involved in NCHC's Grid Computing Resources.
- Users of domestic Grid-based Applications / Projects.
- Foreign collaborators or institutes related to NCHC Grid research.

Certificate Type

- Client Certificate: Client authentication (SSL) under the grid computing environment.
- Server Certificate:
  - Globus server authentication.
  - Access Grid / Conference server authentication.
  - Sensor Net server authentication.
  - Unicore server authentication.
  - LDAP server – Access to LDAP server.

Identification and Authentication

- Users from NCHC:

  Staff members will be identified by inspection of their badge IDs with photos on them. Inspection will take place in person by the user administrator.

- Users from other participating organization:

  Users will be identified through in-person interview by the user administrator. Photo-id or valid official documents must be presented at the interview.

Certificate Restrictions

- Certificate Lifetime:
  - NCHC CA root certificate – 10 years
  - End entity – 1 year

Certificate Revocation

- The user's private key is lost or suspected to be compromised.
- The information in the user's certificate is suspected to be inaccurate.
- The user violates his/her obligation specified in section 2.1.3.
- The CA private key is compromised.

Procedure for Revocation Request

- The RA confirms a revocation request by the client certificate.
- The RA server sends a revocation request to the CA server.
- The CA server will revoke the certificate and update the signed CRL in the repository.

CRL

- NCHC CA will process revocation as soon as it receives the request.
- The information of revocation will be posted in the repository.
- The CRL is valid for 30 days.
- The CRL will be reissued at least 7 days before expiration.
- A relying party can verify a certificate by retrieving the newest CRL published in the repository.

Physical Security

- CA server:
  - dedicated machine.
  - located at a locked room and physical access to the room is restricted to explicitly authorized person.
- CA private key:
  - protected by HSM compliant with FIPS140-1 Level 3.
  - The backup will be saved in the HSM token and stored in a safe place. Backup is made by the CA manager and CA operation staff.

Records Archival

- All certificates and the CRL issued by the NCHC CA
- All enrollments submitted by users and any notifications sent to users.
- All records related to the CA key.
- All the logs as specified in section 4.5.1. (access, issue, revocation, login, logout, reboot, error…).
- All auditing records.
- This CPS and operational procedures documents.
- Other important materials related to decisions of the NCHC PMA.
- Archived data will be stored for 3 years.
- Archive data will be protected in a safe box with appropriate entry control.

Key Pair

- CA Key: The CA Key pair is generated by the operation staff using Hardware Security Module (HSM).
- User Key: The User key pair is generated by software in each user's hardware.
- For client certificate the key size is 1024 bits (RSA).
- For server certificate the key size is 1024 bits (RSA).
- NCHC CA key length is 2048 bits (RSA).

Contact Information

- Tsung-Ying Wu (Alex)
- Grid Operation Center (GOC), NCHC
- 7, R&D Rd. VI, Hsinchu Science Park, Hsinchu 300, Taiwan.
- Phone: + 886-3-5776085#287
  Fax: + 886-3-5776082
  Email: alex@nchc.org.tw