IHEP GRID CA

Gang CHEN, Gongxing SUN

Institute of High Energy Physics

EUGridPMA meeting, Tallinn

2005-6-20

Introduction

- IHEP CA is established and managed by Computing Center of Institute of High Energy Physics (IHEP) in Beijing, since July 2004.
- It provides X.509 certificate to high energy physics community in China.

CP/CPS

- **This document is based on following sources:**

  RFC 2527, CERN CP/CPS,
  CNRS Grid-FR CP/CPS

- **Object ID:** 1.3.6.1.4.1.16796.10.1.1.2
  Version 1.2, April 27 2005

End Entity

- **Natural person, computer and service:**
  - Chinese HEP Users: Domestic individuals participating in high energy physics research
    - IHEP, CNIC, Peking Univ., Shandong Univ., Nanjing Univ., USTC, HUST, ...
  - Chinese HEP computers/services:
    - Computers of domestic Grid-based applications/ projects.
    - Services of Domestic Grid-based Application/Projects, managed by Chinese persons, and running on Chinese computers.

Certificate Type

- **User Certificate:**

  C=CN, O=HEP, OU=IHEP, CN =Sun Gongxing

- **Grid host:**

  C=CN, O=HEP, OU=IHEP, CN=host/host1.ihep.ac.cn

- **Grid Service:**

  C=CN, O=HEP, OU=IHEP, CN=ldap/host1.ihep.ac.cn

Identification and Authentication

- User certificate:
  - Subscriber must meet in person with the IHEP RA. And the user is well known to IHEP RA.
  - IHEP RA must check by phone or conversation that the request originated at the known user.
- Host and service certificate:
  - Requests must be signed by a valid personal IHEP CA user certificate,
  - RA will check meet in person or check by phone to confirm the originator of the request.

Certificate Restriction

- Certificate Lifetime for
  - IHEP CA root certificate is 10 years,
  - End entity is 1 year.

- User certificate should not be shared.

Certificate Revocation

- Circumstances for Revocation
  - subscriber's private key is lost or suspected to be compromised,
  - information in the subscriber's certificate is suspected to be inaccurate,
  - subscriber no longer needs the certificate to access Relying Parties' resources,
  - subscriber has violated his/her obligations.

Procedure for Revocation Request

- The entity requesting revocation of a certificate must authenticate themselves in one of the following ways:
  - From the public IHEPCA web site, submit revocable reasons with CRIN to the IHEP RA.
    If the entity lost CRIN, the request must signed it by an IHEP CA certificate,
  - Contacting the IHEP CA or RA, who will check the entity using the same procedure as certificate request.

CRIN-Certificate Revocation Identification Number: sent to user when issuing certificate

CRL

- CRL is issued immediately after every certificate revocation,
- Valid for 30 days,
- CRL is reissued 7 days before expiration even if there have been no revocations.

Physical Security

- The CA signing machine is
  - A dedicated machine
  - Not connected to any network
  - Locate in a secure room restricted to authorized personnel
  - Have private key and pass phrase stored in USB flash drive.

Records Archival

- The following events are recorded and archived:
  - certificate requests
  - approved certificate requests
  - issued certificates
  - certificate revoke requests
  - issued CRLs
  - Boots and shutdowns of CA machines
- E-mails sent and received by CAs
- Archives are stored in a room with restricted access
- The minimum retention period is 3 years.

Key Pair

- Users use IHEP CA public web UI to create their key pairs as part of the request generation process,
- CA and RA will never generate private keys for users,
- CA and RA have no access to the users' private keys.
- Key size:
  - For End entity: 1024 bits
  - For root certificate: 2048 bits

Contact Information

SUN, Gongxing
Mail Box: PO BOX 918-7, Beijing 100049, China
Phone: +86-010-88236004
Fax: +86-010-88236839
email: gridca@ihep.ac.cn
Address: 19B, Yuquan Road, Shijingshan District, Beijing 100049, China