



Academia Sinica Grid Computing Certification Authority (ASGCCA)

C.C.Chang
Academia Sinica Computing Centre



Outline

- Introduction to ASGCC / ASGCCA
- Procedural Security
- Physical Security
- Technical Security
- Contact Information
- Related Information



Academia Sinica Grid Computing Centre (ASGCC)

- Based in Academia Sinica, one of the foremost research institute in Taiwan.
- Provides Grid-based service, support and e-Science application development for Academia Sinica and its collaboration institutes
- Fosters Grid computing and e-Science application in Taiwan, Asia.



Academia Sinica Grid Computing Certification Authority (ASGCCA)

- The ASGCCA is established and managed by Academia Sinica Grid Computing Centre in Taiwan and has been running since July 2002.



Procedural Security

- End Entity and Certificate Type
- Identification and Authentication
- Certificate Request
- Certificate Revocation
- Records Archival



End Entity and Certificate Type

- End Entities:
 - Users of Academia Sinica Computing Centre
 - Users of Domestic/International Grid-based Application/Projects
- Certificate Type
 - User Certificate
C=TW, O=AS, OU=CC, CN=Yuan Tein Horng /
emailAddress=yth@beta.wsl.sinica.edu.tw
 - Host Certificate
C=TW, O=AS, OU=CC, CN=beta.wsl.sinica.edu.tw
 - Service Certificate
C=TW, O=AS, OU=CC, CN=FTP/beta.wsl.sinica.edu.tw



Identification and Authentication

- User certificate:
 - Academia Sinica Staff:
 - Subscriber must be already registered at the Academia Sinica Grid Computing Directory Service (ASGCDS) as a user defined in end entities.
 - RA staff will check account registered on ASGCDS and contact subscriber personally.
 - International Collaborator:
 - Subscribers fax the certificate application form
 - RAs will verify / confirm the identity of subscriber with project collaborators.
 - RAs confirm / approve the user application to CA administrator.
 - Subscribers apply for certificate via ASGCCA website, user private key generated by users' browser and CSR generated & saved by ASGCCA web server.
 - CA administrator signs the CSR and sends the issued certificate.
- Host or service certificate:
 - Requests must be signed with a valid personal ASGCCA certificate
 - RA will check the FQDN of the host before issuing certificate



Certificate Revocation

- Circumstances for Revocation
 - The entity's private key is lost or suspected to be compromised.
 - The information in the entity's certificate is suspected to be inaccurate.
 - The entity requests for revocation.
 - The entity violates its obligations.



Procedure for Revocation Request

- The person requesting the revocation of certificate must authenticate himself in one of the following ways:
 - sending an email, signed by a valid and trusted certificate, to asgcca@grid.sinica.edu.tw, RA will contact subscriber for confirmation.
 - In the other cases, authentication is performed with the same procedure used to authenticate the identity of person.



Records Archival

- RA must record and archive
 - All requests (including application forms)
 - All confirmations
- CA must record and archive
 - All requests for certificates
 - All issued certificates
 - All requests for revocation
 - All issued CRLs
 - Login/Logout/Reboot of the issuing machine
- All archive data is stored and backed-up in safekeeping.
- The retention period for archives is 3 years



Physical Security

- The CA issuing machine is
 - a dedicated machine
 - not connected to any network
 - located in Academia Sinica computing room, access to the room will be recorded and accompanied by room administrator.
 - ASGCCA private key and pass phrase stored and locked in a safe



Technical Security

- Key Generation
- Key Restriction
- Certificate Restriction
- CRL Policy



Key Generation

- Private key is generated by browsers on the users' machine.
- CA and RA will never generate private key on user's behalf.
- CA and RA have no access to the users' private key.



Key Restriction

- Key Length
 - ASGCCA private key is 2048 bits
 - User private key must have at least 1024 bits
 - Host private key must have at least 1024 bits
 - Service private key must have at least 1024 bits
- Pass phrase
 - The pass phrase of CA's private key is at least 15 characters
 - The pass phrase of end entity's private key is at minimum 12 characters.
 - Protecting the pass phrase from others



Certificate Restriction

- Certificate Lifetime for
 - ASGCCA certificate is 5 years
 - user certificate is one year
 - host certificate is one year
 - service certificates is one year
- User certificate should not be shared.



CRL Policy

- The lifetime of CRL is 30 days
- CRL is updated immediately after every revocation
- CRL is reissued 7 days before expiration even if there have been no revocations



Certificate Statistics

	User Certificate	Host Certificate	Service Certificate	Total
Issued	91	146	3	228
Effectuated	40	84	3	173
Revoked	51	62	0	55

Last update: Thu Oct 20 04:03:46 CST 2005

<http://ca.grid.sinica.edu.tw/publication/status.html>



Contact Information

Contact Person: Yen, Eric

Mail Box: Nankang PO BOX 1-8 Taipei, Taiwan 11529

Address: 128, Sec. 2, Academia Road, Nankang, Taipei, Taiwan 11529

Phone: +886-2-2789-9494

Mobile: +886-922-959211

Fax: +886-2-2783-6444

email: asgcca@grid.sinica.edu.tw



Related Information

- Homepage
 - <http://ca.grid.sinica.edu.tw>
- CP/CPS
 - Latest version: 1.5
 - OID: 1.3.6.1.4.1.5935.10.1.1.5
 - Follows the RFC 2527 structure
 - <http://ca.grid.sinica.edu.tw/CPS/>
- ASGCCA certificate
 - <http://ca.grid.sinica.edu.tw/ASGCCA.crt>
- CRL
 - <http://ca.grid.sinica.edu.tw/CRL/>



The End