

SINAPAD Grid PKI

1st Meeting - TAGPMA

Bruno Schulze

**Coordenação de Ciência da Computação
Laboratório Nacional de Computação Científica**

E-mail: `schulze@lncc.br`

Luiz Gadelha Jr.

**Coordenação de Sistemas e Redes
Laboratório Nacional de Computação Científica**

E-mail: `lgadelha@lncc.br`

Overview

- About SINAPAD
- About GRADGIGA
- Installation environment
- Certification Authority
- End-entity certificates
- Enrollment
- Revocation and CRL's
- Public interface
- Future Work

About SINAPAD

SINAPAD stands for *National System for High-Performance Computing*.

<http://www.lncc.br/sinapad>

It is composed of 7 HPC centers (CENAPAD's) across Brazil, targeting universities and research centers.

LNCC was assigned by the MCT (Min. of Science and Technology) as the coordinator of SINAPAD.

About SINAPAD



About SINAPAD

Sample Applications:

- Weather prediction
- Genomics
- Computational physics

Users (2005):

- Federal universities: 60%
- State universities: 27%
- MCT R&D centers: 11%
- Private universities: 2%

About GRADGIGA

A project to set up a computational grid connecting SINAPAD HPC resources.

Two phases:

- Homogeneous grid: *Sun Fire v20z* clusters.
- Heterogeneous grid: incorporating legacy HPC resources.

About GRADGIGA

Software:

- Globus 3.2
- Gridport 3.1
- OpenCA 0.9.2
- MyProxy 1.16

About GRADGIGA

OpenCA used to implement full CA functionality:

- Public interface (enrollment, repository)
- RA
- CA
- Node management (data synchronization)

MyProxy used as repository for proxy certificates used in the Portal.

Installation Environment

Two dedicated servers:

Public interface and RA server:

Debian Linux OS

RA requires SSL client authentication

CA server (offline):

Debian Linux OS

CA requires SSL client authentication

Certification Authority

Single CA issuing end-entity certificates for:

- SINAPAD users
- SINAPAD hosts

Private-key (2048 bits) stored in the CA server hard-disk.

The server is offline and access to the server room is controlled.

Certification Authority

Whole CA system encrypted (incl. private-key) and backed-up to DLT tapes periodically.

Backup symmetric encryption passphrase known to two staff members only.

Subject format:

`CN=Autoridade Certificadora, OU=GRADGIGA, O=SINAPAD, C=BR`

End-entity certificates

GRADGIGA user certificates are used for dynamic delegation through proxy-certificate issuance.

Subject format:

CN=<Full user name>, OU=<Project name>,

OU=<Institution>, OU=GRADGIGA, O=SINAPAD, C=BR

End-entity certificates

GRADGIGA host certificates are used in client to host mutual authentication.

Subject format:

```
CN=host/<FQDN>, OU=<Institution>, OU=GRADGIGA,  
O=SINAPAD, C=BR
```

Enrollment

GRADGIGA user certificate enrollment:

1. User generates key-pair and CSR (PKCS#10) using applet developed by SINAPAD.
2. User sends CSR via e-mail to AC GRADGIGA or paste it in a enrollment form in the public interface.
3. RA operator goes through the validation process.
4. CA operator issues the certificate.

Enrollment

GRADGIGA host certificate enrollment:

1. System administrator generates key-pair and CSR using `grid-cert-request`.
2. System administrator sends CSR via e-mail to AC GRADGIGA or paste it in a enrollment form in the public interface.
3. RA operator goes through the validation process.
4. CA operator issues the certificate.

Revocation and CRL's

Certificate may be revoked in the following ways:

1. PIN-based revocation in the public interface requested by the user, approved by the RA operator and performed by the CA operator.
2. Direct revocation requested and approved by the RA operator and performed by the CA operator.

Revocation and CRL's

CRL's are issued with a 30 days validity period whenever a certificate is revoked or one day before the current CRL expiration.

Public Interface

The public interface serves as a repository via HTTP for the following data:

- End-entity certificates.
- CRL's.
- CP/CPS (*under construction*).
- CA certificate.

Future Work

Migrate to ICP-EDU software/hardware.

Write CP/CPS documents.

Creation of new RA's in the HPC centers.

Consider compliance with policies presented at TAGPMA.

Thank you!

Questions?