Faculty of Computer Science
scientific computing
universität wien

AustrianGrid CA new architecture

Willy Weisz
University of Vienna
Faculty of Computer Science
Institute of Scientific Computing
VCPC

AustrianGrid Certification Authority

16th EUGridPMA meeting
Zürich, May 11th 2009

Essential changes

Online CA with HSM

- ProtectServer Gold 220
- Certified FIPS 140-2 level 3 (when run in FIPS mode)

New name space

- DC=at,DC=austriangridca
- DNS domain *austriangridca.at* is owned by CA

Hardware preparations for the move

Online CA server in „cage“

- Rack with lock
- Monitored front door opening with finger print
- Back door and side walls monitored
- Temperature monitoring

Memory upgrade

The cage

Software preparations for the move

Virtualisation of the Linux platform

- Xen 3.1
- 1 VM for the running CA
- 2 VMs for development
- 1VM for Windows XP
  - For registering finger prints
  - Monitoring opening of front door – who?
  - Fingerprint reader not working (USB timing problem?)

Hardware

Online CA server

- Repository
- Web server
- One network bridge to public LAN
  - Access restricted to above services
- One network bridge to private LAN
  - Path to online signing server with HSM

Hardware

Online signing server

- With HSM PCI card (ProtectServer Gold 220)
- Single NIC on LAN with private IP address
- Very restricted access

AustrianGrid CA new – User interface

Keys and CSR generated by Java applet

- No need to execute a script
- Support for Windows-only environment
- Java 1.6+ required
  - Supports setting of file access rights
  - Private key
    - User: read only – others: none (Unix: 400)
      - Supports 64bit browsers (not a requirement)

AustrianGrid CA new – User interface

More online checks to guide users

- Check for known vulnerabilities
- Check regeneration if vulnerability discovered

Easier rekey procedure

Automatic migration to new name space when rekeying

User may initiate revocation of certificates when he has access to the private key without RA/CA intervention

AustrianGrid CA new – RA interface

More autonomy and higher responsibility for RA

- RA initiates signing process
  - No CA intervention

Web based interface

- No more e-mail exchange for CSR
  - Reception and
  - Submission

Support for face-to-face meeting

AustrianGrid CA new – RA interface

New name space for RA subjectNames

- O or first OU = *Registration Authorities*

AustrianGrid CA new – next step

After start of operation

Introduction Secure Token

- USB Secure Token
- or (and?) SmartCard
- Documented in certificate
- In addition to key pairs stored on mass storage