Karlsruher Institut für Technologie

GridKa-CA update

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

Outline

About KIT

Main changes to CP/CPS

Minor changes

About KIT

Karlsruhe Institute of Technology – KIT (Germany)

includes the former Forschungszentrum Karlsruhe in der Helmholtzgemeinschaft (FZK) and University of Karlsruhe aim is to combine research and education (...)

One institute of KIT is the Steinbuch Centre for Computing – SCC which is the computing centre and was formerly called 'Institute for Scientific Computing' (IWR)

Tier 1 centre for LHC (GridKa)

Many grid/clouds projects (EGI-inspire, D-Grid,..)

Major change 1 - Name

Name changes within the Policy

FZK -> KIT

IWR -> SCC

Mail address/general contact information changed:

'gridka-ca@iwr.fzk.de'-> 'gridka-ca@kit.edu'
(root certificate includes old address, mails to the old address will still be accepted and forwarded)

GridKa-CA is now run by SCC at KIT (but still from the same people)

Major change 2 – robot certs

Want to issue robot certs with private key protected in files

1.3.3 End entities ~ robot certs are issued

3.1.1 Types of names

„CN must start with the string „Robot: grid function“ followed by „- first name surname“ of the subscriber”

7.1.6 Certificate policy Object Identifier

„Robot certificates include the 1SCP robot OID.“

Major change 2 – robot certs

6.2 Private Key protection

"Robot, host and service certificates may be stored in unencrypted form. The responsible person shall protect the private key via appropriate file-system-level protection, such that only the person or group of persons responsible for the service or host has access to this key. The subscriber is and must be responsible for the host in which the credentials are installed, and must be responsible for granting and revoking privileged access to the file system by others."

Major change 2 – robot certs

7.1.2 Certificate extensions - Robot Certificates

Subject Key Identifier: unique identifier of the subject (hash)

Authority Key Identifier: unique identifier of the issuer

Subject Alternative Name: subject's e-mail address or FQDN

Issuer Alternative Name: issuer's e-mail address

CRL Distribution Points: URI:http://grid.fzk.de/ca/

Certificate Policies: The OID of the CP/CPS (OID 1.3.6.1.4.1.2614.5548.1.1.1.6), OID referring to the IGTF Profile for „Classic X.509 Certification Authorities with secured infrastructure“ (OID 1.2.840.113612.5.2.2.1), OID of the IGTF profile for robot certificates with Private Key protection: Key material held in files (OID 1.2.840.113612.5.2.3.1.2)

Netscape Cert Type: SSL Client, S/MIME

Netscape Comment: CP/CPS version

Netscape Base Url: http://grid.fzk.de/ca

Netscape Revocation Url: http://grid.fzk.de/ca/gridka-crl.der

Netscape CA Policy Url : http://grid.fzk.de/ca/gridka-cps.pdf

Major change 3 - Identification process

Former practice:

personal contact, taking copy of identity card

Now new identity cards in Germany with sensitive information on it – copies not allowed anymore

see section 3.1.9

We need to have a registration form with name, surname, date and place of birth, last five numbers of id card

Minor changes

Adapted structure to be conform with RFC 2529

(many new paragraphs, but no substantial changes)

Formatting

Better wording and better descriptions in many many cases
(see email)

Issue crl version 2

End

Happy to receive comments

(already fixed many typos after comments from Bob Cowles and Miroslav Dobrucky - Thanks)

Links

KIT http://kit.edu

SCC http://scc.kit.edu

GridKa-CA http://grid.fzk.de/ca and
https://gridka-ca-sec.fzk.de