Spanish e-Science CA

pkIRISGrid CA Self Audit

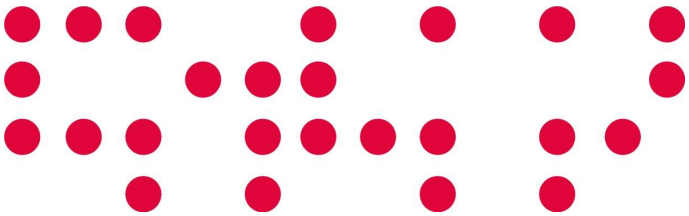
Javi Masa - javier.masa@rediris.es

red.es

Red IRIS

EUGridPMA meeting, Dublin, 2010

Index



- PKI for e-science activities provided by the Spanish NREN RedIRIS
- pkIRISGrid Certification Authority
  - Classic CA Profile
  - Accredited in Vienna 2006
- Initial lifetime
  - 10 years, until June 2015
- Software
  - pkIRIS 0.8.5

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- 41 RAs
  - 22 Universities
  - 19 Research institutes
- 18 locations
- Each RA has
  - 1 administrator
  - 1 or more operators
- Staff
  - 101 RA staff in database
  - 3 CA staff

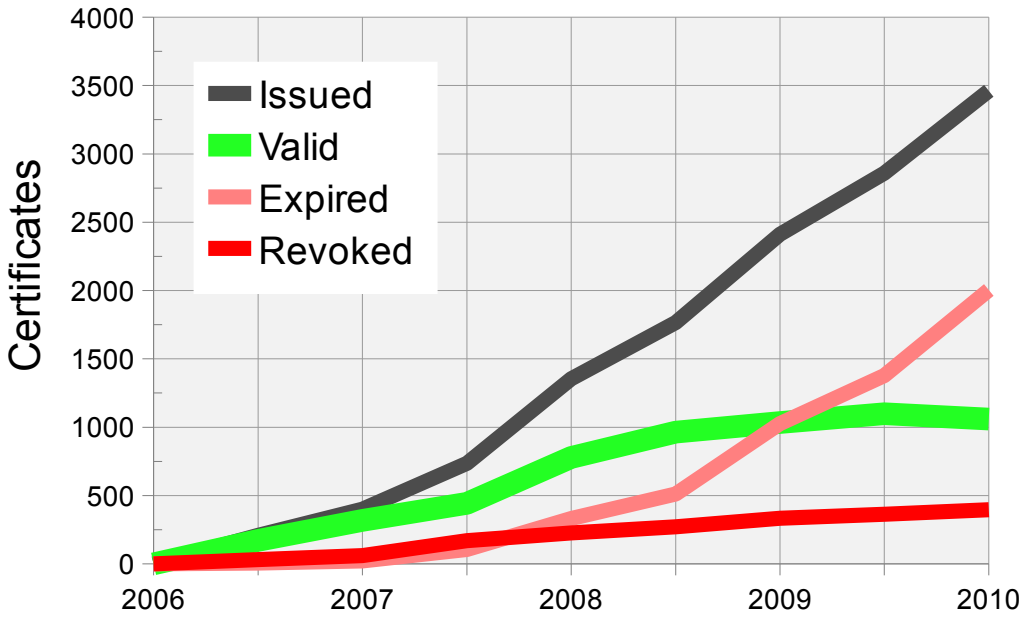
RedIRIS

pkIRISGrid Status
Certificates and CRLs up to 15/01/2010

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- 3480 certificates issued
  - 1449 users
  - 2031 host/services
- 1062 currently valid
  - 432 distinct users
  - 630 distinct hosts
- CSRs
  - Generated via web browser
- 192 issued CRLs



RedIRIS

- Using an unofficial version of the Auditing Guidelines Document
  - Sent to the list on 2009-11-11

- (8) The CA system must be located in a secure environment where access is controlled
  - How is the access log recorded?
    - The CA operator manually put his name and timestamp in a paper notebook
    - **We are considering how to improve the procedure**

- (16) The on-line CA architecture should provide (**preferably tamper-protected**) log of issued certificates and signed revocation lists
  - All logs of issued certificates are stored in LDAP DB
  - Logs lines are SHA1 signed
  - Is this log tamper-protected?
    - Not against item deletion
    - **Tamper protection could be improved**

Self Audit Results: Bs - 3
(minor changes)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (22) The profile of the CA certificate must comply with the Grid Certificate Profile as defined in GFD.125
  - extendedKeyUsage is not part of the CA certificate but it is mentioned in our CP/CPS
    - **We need to correct our CP/CPS**

Self Audit Results: Bs - 4
(minor changes)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (24) The CA must react as soon as possible, but within one working day, to any revocation request
  - We usually react within one day but our CP/CPS says:
    4.9.5. *The pkIRISGrid CA must process revocation request with the highest priority*
    - **We will update our CP/CPS**

Self Audit Results: Bs - 5
(minor changes)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (25) Subscribers must request revocation of its certificate as soon as possible …
  - Subscribers are warned about this obligation when requesting a certificate
  - The obligation is not reflected in our current CP/CPS
    - **Need to update 4.9.1 in our CP/CPS**

- (37) … subscribers must protect theirs private keys
  - Subscribers are warned about this obligation when requesting a certificate
  - The obligation is not reflected in our current CP/CPS
    - **We need to add some text to our CP/CPS related to the protection of private keys**
    - **Where in the CP/CPS?**

Self Audit Results: Bs - 7
(minor changes)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (47) Every CA must perform operational audits of the RA staff at least once per year
  - It's very complicated (>100 people)
  - Each RA signs a document that declares their operational procedures
    - including items related to RAs from “Guidelines for auditing Grid CAs”
  - Meetings twice a year
  - But we cannot guarantee to audit every RA every year
    - Expensive in time and money

Self Audit Results: Cs
(major changes)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (42) Certificates must not be renewed or re-keyed consecutively for more than 5 years … (without a F2F meeting with RA)
  - pkIRISGrid CA started in January 2006 (4 years)
    - So we have had no opportunity to infringe this
  - But
    - **We have to include this in CP/CPS**
    - **Modify our software to enforce this**
    - **3 is a good number**

Self Audit Results: Ds
(must change)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (40) Certificates ... managed in a software token should only be re-keyed ...
  - Web browser generates private keys
    - The first time a certificate is requested
    - After a revocation and a request with the same DN
  - But when a certificate is renewed we use the same CSR stored in our DBs
    - **We are modifying the renew procedure to do a re-key and generate a new CSR**

Self Audit Results: Xs
(could not evaluate)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- (41) … private key residing solely on hardware token may be renewed for a validity period of up to 5 years …
  - We don't provide specific support for hardware tokens
  - We do the same as in (40)

- Results
  - 7 Bs - Recommendation (minor change)
  - 1 C - Recommendation (major change)
  - 1 D - Advive (must change)
  - 1 X - Could not evaluate (N/A)
- Conclusions
  - We are on the right way
  - We need to review our CP/CPS
  - We need to write a few lines of code

Questions?

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO
red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es

RedIRIS. Edificio CICA
Avenida Reina Mercedes s/n
41012. Sevilla. España

Tel: 95 505 66 00
Fax: 95 505 66 27
www.rediris.es

RedIRIS