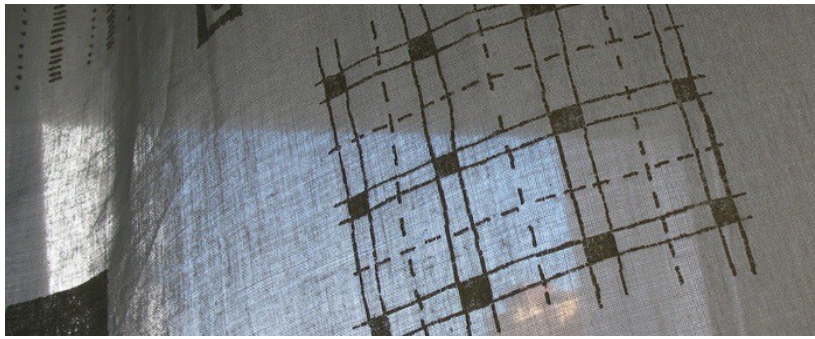
pkIRISGrid CA
update & selft-audit results

Spanish e-Science CA

Javi Masa - javier.masa@rediris.es

Overview

1. **pkIRISGrid CA**
2. Statistics
3. Latest operational changes
4. CP/CPS update
5. Self Audit
6. Further plans



pkIRISGrid
General information

- pKIRISGrid is an X.509 PKI with offline CA infrastructure
  - PKI for e-science activities provided by the Spanish NREN RedIRIS
- pkIRISGrid Certification Authority
  - Classic CA Profile
  - Accredited in Vienna 2006
  - Works from Seville
- Initial lifetime
  - 10 years, until June 2015
- Software
  - OpenSSL
  - pkIRIS (perl + PHP)

Overview

1 pkIRISGrid CA

2 **Statistics**

3 Latest operational changes

4 CP/CPS update

5 Self Audit

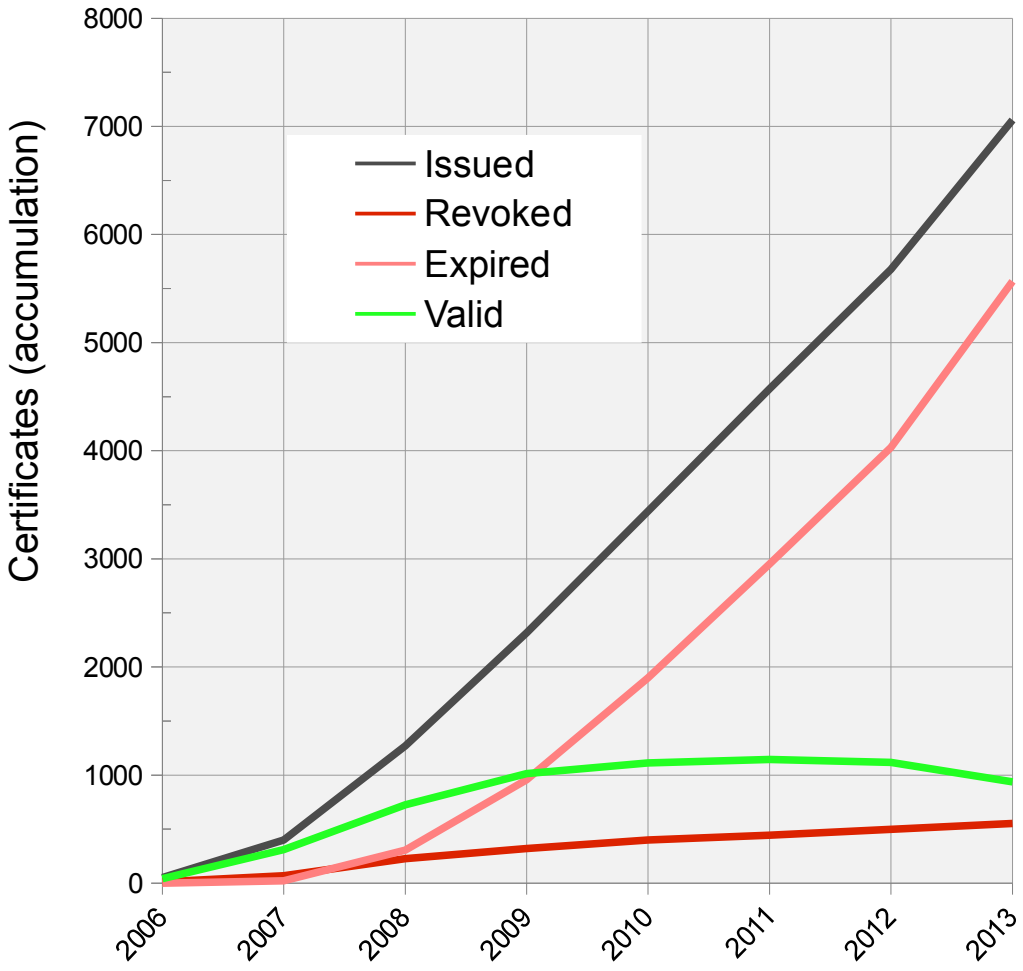
6 Further plans

pkIRISGrid - statistics
Up to 01/05/2013

- 47 RAs
  - 29 Universities
  - 18 Research Institutes
- 20 locations
- Each RA has
  - 1 administrator
  - 1 or more operators
- Staff
  - 118 RA staff
  - 2 CA staff

pkIRISGrid - statistics
Certificates and CRLs up to 01/05/2013

- 7058 certificates issued
  - 3107 users
  - 3951 hosts/services
  - 1 robot
- 938 currently valid
  - 447 unique user certs
  - 491 unique host certs
  - 1 robot certificate
- CSRs
  - 7595 Generated via web browser (user/host/srv)
  - 1 robot (openSSL)
- 303 issued CRLs



Overview

1. pkIRISGrid CA
2. Statistics
3. **Latest operational changes**
4. CP/CPS update
5. Self Audit
6. Further plans

Latest operational changes

2010

- 2 new RAs (total RAs = 44)
- New offline USB HDD for backups

2011

- 2 new RAs (total RAs = 46)
- HW upgrade:
  - New CA computer (laptop)
  - New USB key for CA private key
    - The old USB key was physically destroyed
- 1 less CA Operator

Latest operational changes

2012

- Robot profile
- SHA2 operational
  - 5 issued certs for testing purpose
- CP/CPS: CRRs issued within one working day instead of “on best effort”
- 1 new CA Operator

2013

- 1 new RA (total = 47)
- 14 SHA2 issued certs for testing purpose
- 1 robot cert issued
- Changed Link to CRL from PEM to DER in issued certificates
- 1 less CA Operator

Overview

1. pkIRISGrid CA
2. Statistics
3. Latest operational changes
4. **CP/CPS update (2010-)**
5. Self Audit
6. Further plans

CP/CPS mayor changes

- Added “Classic X.509 Certification Authorities with Secured Infrastructure” OID
- CRL is no longer registered by LDAP
- Added information about circumstances for certificate re-key and explain in detail identification and authentication for routine re-key
- Added method to prove possession of private key (3.2.1)
- The pkIRISGrid CA must process revocation requests within 1 working day
- 7.1.2 Certificate extensions. A lot of changes, overhaul of this section with extensions featured in table format
- Added a new certificate profile for robot. Modified a lot of sections
- Added the option to include a dash in the CN component of a natural person certificate (3.1.1, 3.1.4)
- Publishing pending: Changed Link to CRL from PEM to DER in issued certificates (cRLDistributionPoints)

CP/CPS changes

v 1.1.4 - January 13, 2010

7.1.6
- Added “Classic X.509 Certification Authorities with Secured Infrastructure” OID 1.2.840.113612.5.2.2.1
- Added reference to GFD-C.125 Grid Certificate Profile

v 1.1.5 - January 20, 2012

6.7 Removed “It has not any network adapter”

7.1 *CRL is no longer registered by LDAP*

v 1.2.0 - May 02, 2012

4.6 Correction of the renewal section

4.7.1 Added information about circumstances for certificate re-key

4.9.1 Subscribers must request revocation in some cases

CP/CPS Changes

v 1.3.0 - October 30, 2012

1.2 Added CP/CPS download URL http://pki.irisgrid.es/ca/policy

1.3.1 Added additional details about the running of pkIRISGrid CA

3.2.1 Added *method to prove possession of private key*

3.2.3 Changed to accept personal identity documentation in the EU

3.3.1 Explain in detail identification and authentication for routine re-key

3.3.2 Changed "Re-key after revocation follows the same rules as an initial registration"

4.7.1 Now describes the 3 common cases for re-keying certificates

4.9.5 Now "The pkIRISGrid CA must process revocation requests within 1 working day"

5.1.1, 5.1.2 Modified sections in order to give additional data and reorganize the current information between these two related sections about physical protection

5.1.4 Added "No water-cooled systems are used and there are no water pipes or water sources near the CA."

5.5.1 Added details about the logs:
"All logs of issued certificates are stored in LDAP DB and logs lines are signed."

CP/CPS Changes

7.1.2 Certificate extensions.

Overhaul of this section

- *Extensions featured in table format.*
- Removed Netscape Cert Type and Comment from natural person and server certificates. Netscape extensions are deprecated.
- Added Subject Alternative Name and Issuer Alternative Name for natural person and server certificates.
  We had them in the CA but not written in the CP.
- Removed timeStamping from user and server certificates. Not needed.
- Removed codeSigning from user and server certificates. Not needed.
- Removed nonRepudiation from user and server certificate following “Grid Certificate Profile” (GWD-R. 125Bis version 5 from June 2012)
- Removed emailProtection from server certificates (not needed) and marked as Optional in user certificates.

Certificate Extension	CA	User	Server	Robot
basicConstraints				
• *critical*	M	M	M	M
• *CA: TRUE*	M			
keyUsage				
• *critical*	M	M	M	M
• *digitalSignature*	M[1]	M	M	M
• *keyEncipherment*		M	M	M
• *dataEncipherment*		M	M	
• *nonRepudiation*	M[1]			
• *keyCertSign*	M			
• *cRLSign*	M			
extendedKeyUsage				
• *clientAuth*		M	M	M
• *emailProtection*		O		M
• *serverAuth*			M	
nsCertType[1]				
• *SSL Certificate Authority*	M			
• *Email Certificate Authority*	M			
• *Object Signing*	M			
nsComment[1]				
• *STRING*	M			
cRLDistributionPoints				
• *URI: http://pki.irisgrid.es/ca/crl/cacrl.pem*	M	M	M	M
authorityKeyIdentifier				
• *KeyID*	M	M	M	M
subjectKeyIdentifier				
• *KeyID (hash)*	M	M	M	M
certificatePolicies				
• *(CP/CPS)*	M	M	M	M
• *(Classic CA) 1.2.840.113612.5.2.2.1*		M	M	M
• *(Robots) 1.2.840.113612.5.2.3.3.1*				M
• *(PKP: file-based) 1.2.840.113612.5.2.3.1.2.1*				M
subjectAlternativeName				
• *URI*		M	M	M
• *EMAIL*		O		M
• *DNS*			M	
issuerAlternativeName				
• *URI: http://pki.irisgrid.es/*		M	M	M

CP/CPS Changes

v 1.4.0 - November 22, 2012

1.3.3	Added a *new certificate profile: robot*
1.4.1	Added the word “robots” to accept authentication of robots
3.1.1	• Added a better example about the CN of personal certificates • Added complete information about the CN of robot certificates
3.1.4	Added detailed information about the form of the CN's in robot certs.
4.1.1	Addded “robots, which are responsibility of a natural person or organization,”
7.1.2	Added robot profile to the certificate extensions table
7.1.4	• Added the name form of the robot certificates: “*Robot - <robot purpose> managed by <owner>*” • Added [ ] and < > description.
7.1.6	Added new two OID's which are being used for robot certificates: • Non human client or robot entity: 1.2.840.113612.5.2.3.3.1 • PKP regarding key material held in files: 1.2.840.113612.5.2.3.1.2.1

CP/CPS Changes

v 1.4.1 - February 04, 2013

3.1.1, 3.1.4

- Added the option to include a dash in the CN component of a natural person certificate.
- Changed the default example for a natural person to better understand the rules.
- Fixed errata: “natural personal” -> “natural person”

9.12.2 Added “Users will not be warned in advance of changes made to the pkIRISGrid CA CP/CPS”.

v 1.4.2 – (publishing pending)

3.3.1 Added “Remember the subject must be an e-science project member”

7.1.2 Changed Link to CRL from PEM to DER in issued certificates (cRLDistributionPoints)

Overview

1. pkIRISGrid CA
2. Statistics
3. Latest operational changes
4. CP&CPS update
5. **Self Audit**
6. Further plans

Self-Audit
Last audit

- Last audit
  - Dublin, January 2010
- Auditing Guidelines document
  - Used an unofficial 1.0 version of the Auditing Guidelines Document (Sent to the list on 2009-11-11)
- Summary
  - 1 X - Could not evaluate (N/A)
  - 1 D - Advive (must change)
  - 1 C - Recommendation (major change)
  - 7 Bs - Recommendation (minor change)

Self-Audit
May 13, 2013

- Auditing Guidelines document
  - Using GFD.169 - 1.1 version (2010-10-28)
- Summary
  - 1 X - Could not evaluate (N/A)
  - 4 (A/B)s

Self Audit - (8)

- (8) The CA system must be located in a secure environment where access is controlled - (A/B)
  - Access to the building
    - Access is controlled by security personnel
    - 24H closed-circuit television (CCTV)
    - Also includes safety arcs for metals
  - Access to the CA room
    - Is done using a key (CA oper, security personal/maintenance)
  - Access to the CA computer
    - Stored in a safe when not in use
    - Access to the box is done using numeric password
    - How is the access log recorded?
      - CA operator manually put his name, sign, timestamp and operations done in a paper notebook

Self Audit - (16)

- (16) The on-line CA architecture should provide (preferably tamper-protected) log of issued certificates and signed revocation lists
  - Last audit (B):
    - All logs of issued certificates are stored in LDAP DB
    - Logs lines are SHA-1 signed
    - Is this log tamper-protected?
      - Not against item deletion (**Tamper protection could be improved**)
  - Now (A):
    - New logs lines are SHA-2 signed
    - New SHA-2 checksum using all log lines related to one certificate
    - Is this log a better tamper-protected log?
      - We think yes :)

Self Audit - (17)

- (17) When the CA's cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes.
  - Last audit (A):
    - We have had no opportunity to infringe this
  - Now (A/B): (CP/CPS publishing pending)

> **5.6 Key changeover**
>
> The following steps SHOULD be taken when re-keying the signing key of the pkIRISGrid CA:
>
> - A new certificate with the new key for the CA SHALL be issued.
> - The new certificate SHALL be published in accordance with Section 2.2.
> - The new certificate is used for issuing certificates. Both the new and the old certificate may be active at the same time. The old key SHALL be used as long as all certificates signed by it have not expired.

Self Audit - (22)

- (22) The profile of the CA certificate must comply with the Grid Certificate Profile as defined in GFD.125
  - Last audit (B):
    - extendedKeyUsage is not part of the CA certificate but it is mentioned in our CP/CPS
  - Now (A):
    - Deleted from CP/CPS

Certificate Extension	CA	User	Server	Robot
basicConstraints				
• *critical*	M	M	M	M
• *CA: TRUE*	M			
keyUsage				
• *critical*	M	M	M	M
• *digitalSignature*	M[1]	M	M	M
• *keyEncipherment*		M	M	M
• *dataEncipherment*		M	M	
• *nonRepudiation*	M[1]			
• *keyCertSign*	M			
• *cRLSign*	M			
extendedKeyUsage				
• *clientAuth*		M	M	M
• *emailProtection*		O		M
• *serverAuth*			M	
nsCertType[1]				
• *SSL Certificate Authority*	M			
• *Email Certificate Authority*	M			
• *Object Signing*	M			
nsComment[1]				
• *STRING*	M			
cRLDistributionPoints				
• *URI: http://pki.irisgrid.es/ca/crl/cacrl.pem*	M	M	M	M
authorityKeyIdentifier				
• *KeyID*	M	M	M	M
subjectKeyIdentifier				
• *KeyID (hash)*	M	M	M	M
certificatePolicies				
• *(CP/CPS)*	M	M	M	M
• *(Classic CA) 1.2.840.113612.5.2.2.1*		M	M	M
• *(Robots) 1.2.840.113612.5.2.3.3.1*				M
• *(PKP: file-based) 1.2.840.113612.5.2.3.1.2.1*				M
subjectAlternativeName				
• *URI*		M	M	M
• *EMAIL*		O		M
• *DNS*			M	
issuerAlternativeName				
• *URI: http://pki.irisgrid.es/*		M	M	M

Self Audit - (24)

- (24) The CA must react as soon as possible, but within one working day, to any revocation request
  - Last audit (B):
    - We usually react within one day but our CP/CPS says:

      4.9.5. Time within which CA must process the revocation request
      The pkIRISGrid CA must process revocation request with the highest priority
    - We will update our CP/CPS
  - Now (A):

    > **4.9.5 Time within which CA must process the revocation request**
    >
    > The pkIRISGrid CA must process revocation requests within one working day.

Self Audit - (25)

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

> **4.9.1 Circumstances for revocation**
>
> Subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of:
>
> - He/she lost or compromised the private key pertaining to the certificate
> - The data in the certificate are no longer valid.

Self Audit - (37)

- (37) … subscribers must protect theirs private keys
  - Last audit (B):
    - Subscribers are warned about this obligation when requesting a certificate but the obligation is not reflected in our current CP/CPS
  - Now (A/B):
    - Subscribers must take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
      - Selecting a strong passphrase;
      - Protecting the passphrase from others;
      - Notifying immediately the IRISGrid CA and any relying parties if the private key is lost or compromised;
      - Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.
    - But in section 4.1.2.
      - Will be changed to section 6.2.8

Self Audit - (40)

- (40) Certificates (and private keys) managed in a software token should only be re-keyed, not renewed
  - Last audit (D):
    - Web browser generates private keys
      - The first time a certificate is requested
      - After a revocation
      - After an expiration
    - But when the certificate is about to expire we use the same CSR stored in our DBs
      - We are modifying the certificate renew procedure to do a re-key and generate a new CSR
  - Now:
    - (See next slide)

Self Audit - (40)

- (40) Certificates (and private keys) managed in a software token should only be re-keyed, not renewed
  - Now (A):
    - Added software to do re-keys and to check compromised keys before issuing certificates
    - Changes in CP/CPS

> **4.6 Certificate renewal**
>
> The pkIRISGrid CA SHALL NOT support certificate renewal. See 4.7 for more information.

> **4.7 Certificate re-key**
>
> 4.7.1 Circumstance for certificate re-key
>
> A certificate re-key will take place in these scenarios:
>
> - *The certificate is about to expire*. See section 3.3.1 for more information.
> - The certificate is expired: follows the same rules as an initial registration.
> - The certificate is revoked: follows the same rules as an initial registration.

Self Audit - (41)

- (41) Certificates associated with a private key residing solely on hardware token may be renewed for a validity period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits).
  - Last audit (X):
    - We don't provide specific support for hardware tokens
  - Now (X):
    - We don't provide specific support for hardware tokens

Self Audit - (42)

- (42) Certificates must not be renewed or re-keyed consecutively for more than 5 years without a form of auditable identity and eligibility verification, and this procedure must be described in the CP/CPS.
  - Last audit - 2010 - (C):
    - 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
  - Now:
    - (See next slide)

Self Audit - (42)

- (42) Certificates must not be renewed or re-keyed consecutively for more than 5 years … (without a F2F meeting with RA)
  - Now (A/B):
    - CP/CPS

> **3.3.1 Identification and authentication for routine re-key**
> Before the certificate expires, and providing that the last identification in accordance to Section 3.2.3 is not older than 5 years, re-key can be done using a secure web interface which checks the validity of the subject's certificate. Expiration warnings will be sent to subscribers 30 days and 7 days before it is re-key time.
> In all the other cases re-keying follows the same rules as an initial registration.

    - Software in process:
      - Checks last F2F identification and if it is older than 5 years
        - Alerts the user when he resquests the new certiticate and
        - Alerts the RA operator for a new F2F meeting to do identity checks

Self Audit - (47)

- (47) Every CA must perform operational audits of the RA staff at least once per year
  - Last audit (B):
    - It's very complicated (>110 people)
    - Each RA signs a document that declares their operational procedures including items related to RAs from “Guidelines for auditing Grid CAs”
    - 2F2 meetings, but we cannot guarantee to audit every RA every year
      - Expensive in time and money
  - Now (A):
    - RA procedure audit
    - RA staff audit
    - RA data audit

Self Audit
(47) operational audits of the RA staff

- RA procedure audit
  - Each RA signs a document that declares their operational procedures including items related to RAs from “Guidelines for auditing Grid CAs”
  - This document must be created before the RA is in production

Self Audit
(47) operational audits of the RA staff

- RA staff audit
  - List of RAs and personnel
    - http://pki.irisgrid.es/ra/select/
  - Meetings
    - Annual F2F meeting
    - Specific meetings
    - Videoconferences
    - Telephone audits
  - Similar to EUGridPMA Private Membership Information
    - http://www.eugridpma.org/members/internal/display/

Self Audit
(47) operational audits of the RA staff

- Data audit
  - 2 certificates audited by RA/year
  - Required documentation
    - User authentication
      - Copy of National Identity Card
    - F2F meeting proof
      - Mail requesting F2F meeting
      - F2F document
    - Relationship with organization
    - Private key proof of possesion

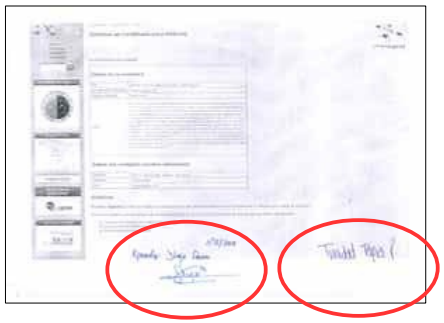
Self Audit
(47) operational audits of the RA staff

- User authentication
  - Copy of National Identity Card (or similar, with photo)
- Face to face meeting proof
  - User and RA operator hand signed

National Identity Card

Mail requesting F2F

F2F meeting



F2F meeting

Self Audit
(47) operational audits of the RA staff

- Relationship with organization
  - A proof that user works for the organization
    - Contract work, institutional identity document, ...
  - Proof that the applicant works in eScience projects
  - Proof that the applicant has control over the server (server certificate)

Relationship with organization

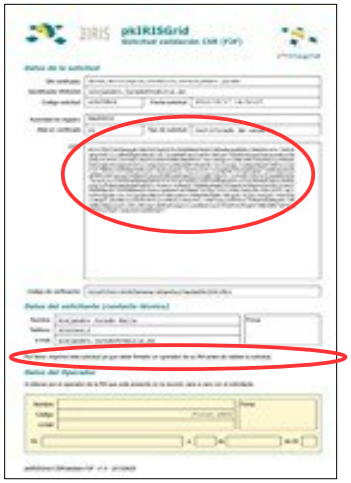
Relationship with eScience

Server control

Self Audit
(47) operational audits of the RA staff

- Private key proof of possesion
  - Before May 2012: Screenshot with the request
  - After May 2012: Document automatically generated after the request

Private key proof of possession
Screenshot



Private key proof of possession
PDF document

Overview

1. pkIRISGrid CA
2. Statistics
3. Latest operational changes
4. CP&CPS update
5. Self Audit
6. **Further plans**

Further plans

- Update CP/CPS
- Finish some software features
- Web:
  - Finish English version
  - Update web user manual
- Create our compromise and disaster recovery document
  - RedIRIS/Seville and the pkIRISGrid CA is located inside a building that is part of governmental facilities for research and higher education. The plans for business continuity and disaster recovery for governmental activities related to research and education are applicable.
- Add IPv6 support for CA web
- OCSP responder

Thanks for your attention

Red IRIS

25 years helping R&D in Spain