



5th EUGRidPMA meeting in Poznan,
September 28-30 2005

# pkIRISGrid

## a PKI for e-science activities provided by the Spanish NREN RedIRIS

Javi Masa, RedIRIS


- Policy
  - CP/CPS status
  - EUGridPMA minimum requirements
- Technology
  - pkIRISGrid architecture
  - Technology used
    - LDAP, COPA, URN, XML, ...
- Certificate enrollment process
  - Sample
- Future plans

# pkIRISGrid CP/CPS status



- CP/CPS document is based on
  - RFC 3647
- Current Object ID:
  - 1.3.6.1.4.1.7547.2.2.4.1.0.0
  - Version: 1.0.0 beta – September 21, 2005
- Available
  - at the EUGridPMA site
  - http://www.irisgrid.es/pki/

- Is our policy compliant with the EUGridPMA minimun requirements?

# pkIRISGrid CA - EUGridPMA
## Minimum requirements - v3.2 (02/02/2005) - 1/5



- CA physical security controls
  - Dedicated offline machine
  - Without network adapter
  - It is switched off between signing operations
  - Laptop stored in a non-flammable vault when not in use
  - Certificates and keys stored in USB sticks in vault
  - Physical access is restricted to pkIRISGrid CA operators
- Namespace: DC=es, DC=irisgrid
  - DC=es, DC=irisgrid, CN=IRISGridCA
  - DC=es, DC=irisgrid, [O=string,] CN=**name@name.es**
  - DC=es, DC=irisgrid, [O=string,] CN=FQDN
  - DC=es, DC=irisgrid, [O=string,] CN=service/FQDN

- written like mail
- NOT MAIL

- User certificates
  - DC=es, DC=irisgrid, CN=rafa.marco @ ifca.es
- Hosts
  - DC=es, DC=irisgrid, CN=grid1.domain.es
- Services
  - DC=es, DC=irisgrid, CN=ldap/machine1.domain.es

- written like mail
- NOT MAIL

- Optional 'O' component can be inserted between 'DC' and 'CN' component
  - DC=es, DC=irisgrid, **O=rediris**, CN=drlopez @ irisgrid.es
  - DC=es, DC=irisgrid, **O=ifca**, CN=rafael.marco @ irisgrid.es

# pkIRISGrid CA - EUGridPMA
## Minimum requirements - v3.2 - 3/5



- DN uniqueness
  - One RA can manage a group of domains
    - @rediris.es, @irisgrid.es, @rediris.com
  - Two equal CNs are not allowed below the same domain
    - pkIRISGrid software does this check when user requests a certificate
- Personal subscriber identification
  - Photo ID
  - PIN inserted when certificate is requested
  - pkIRISGridID obtainded when certificate is requested
- Certificate lifetime
  - pkIRISGrid CA is 10 years
  - End entity is 1 year

- pkIRISGrid CA certificate
  - Private key length is 2048 bits
  - Password length is greater than 16 characters
- Subscriber generates its own key pair (web interface)
  - CA and RA have not access to the user's private key
- Revocation
  - Circumstances
    - Private key lost or suspected to be compromised
    - Subscriber does not need the certificate, ...
  - Who can request them?
    - Owner, RA and CA
    - Any person presenting proof of knowledge that the subscriber's private key has been compromised or data have changed

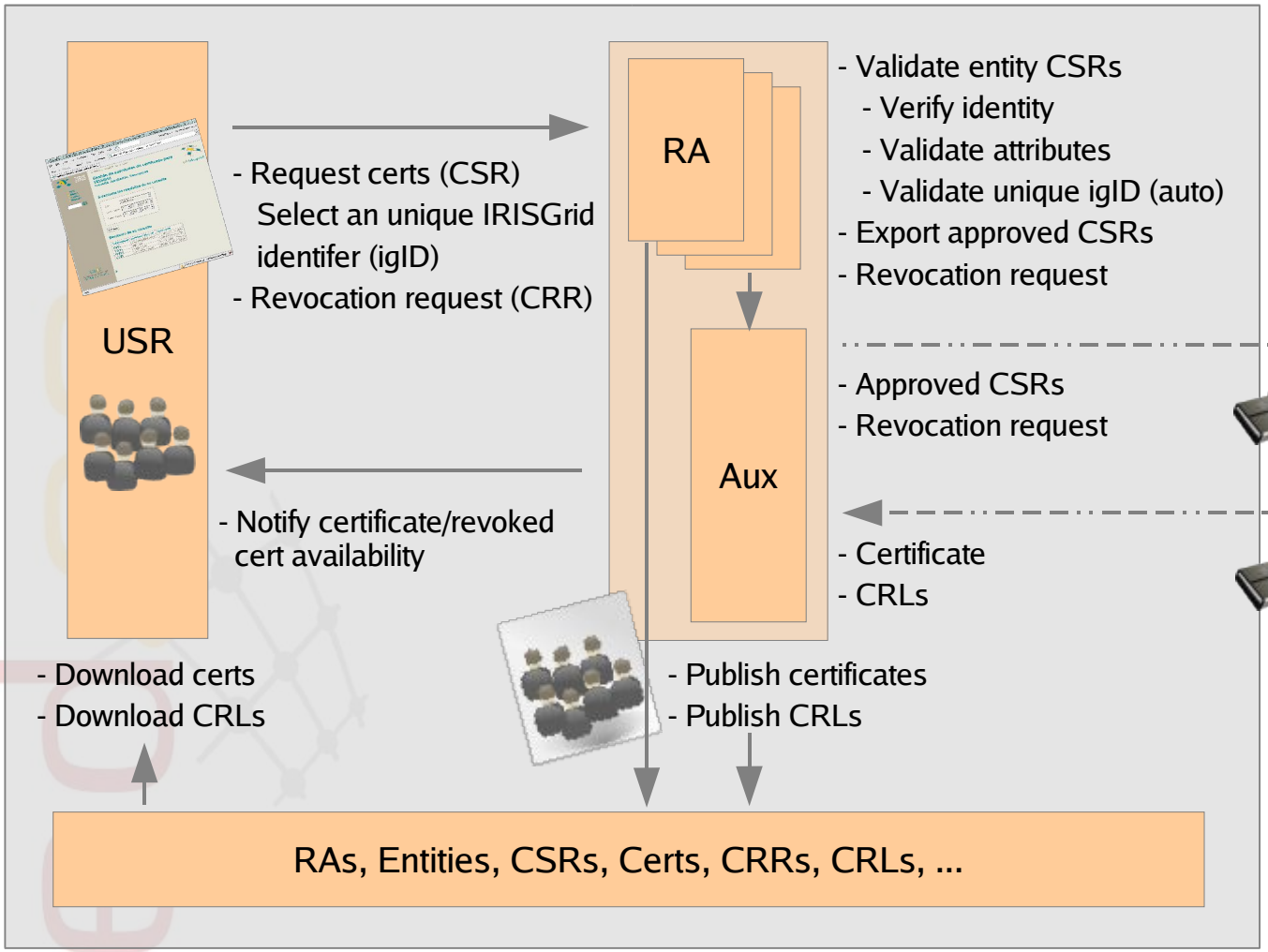
# pkIRISGrid CA - EUGridPMA
## Minimum requirements - v3.2 - 5/5



- CRLs
  - Valid 30 days
  - Includes all revoked certificates
  - Issued immediately after every certificate revocation process
- Policy
  - **1.3.6.1.4.1.7547**.2.2.4.X.X.X - pkIRISGridCA CPS version X.X.X
- RAs hosted by RedIRIS servers (TLS)
  - User interface
    - https://**RAn**.irisgrid.es
  - Administrator interface
    - https://**RAn**.irisgrid.es/**admin**/

# pkIRISGrid. Functional structure





# Technology used by pkIRISGrid



- OpenSSL
- LDAP (pkirisgrid schema)
  - Used to store RAs, entities, CSRs, certificates, logs
- COPA (a coding schema optimized for the hierarchical access to information)
  - **a3b105c1** identify RA 3, entity 105 and CSR/Certificate 1
- URNs
  - Used to store all the states in the life of a certificate
    - urn:mace:rediris.es:irisgrid:pki:csr:state:**20050304**142236:**signed**:10e190a0c7608...2d425e6af7
- XML/LDIF
  - Exchange files between CA and RAs/Aux
- PHP (RAs), Perl (CA)
- PAPI (Access control)

# pkIRISGrid LDAP schema

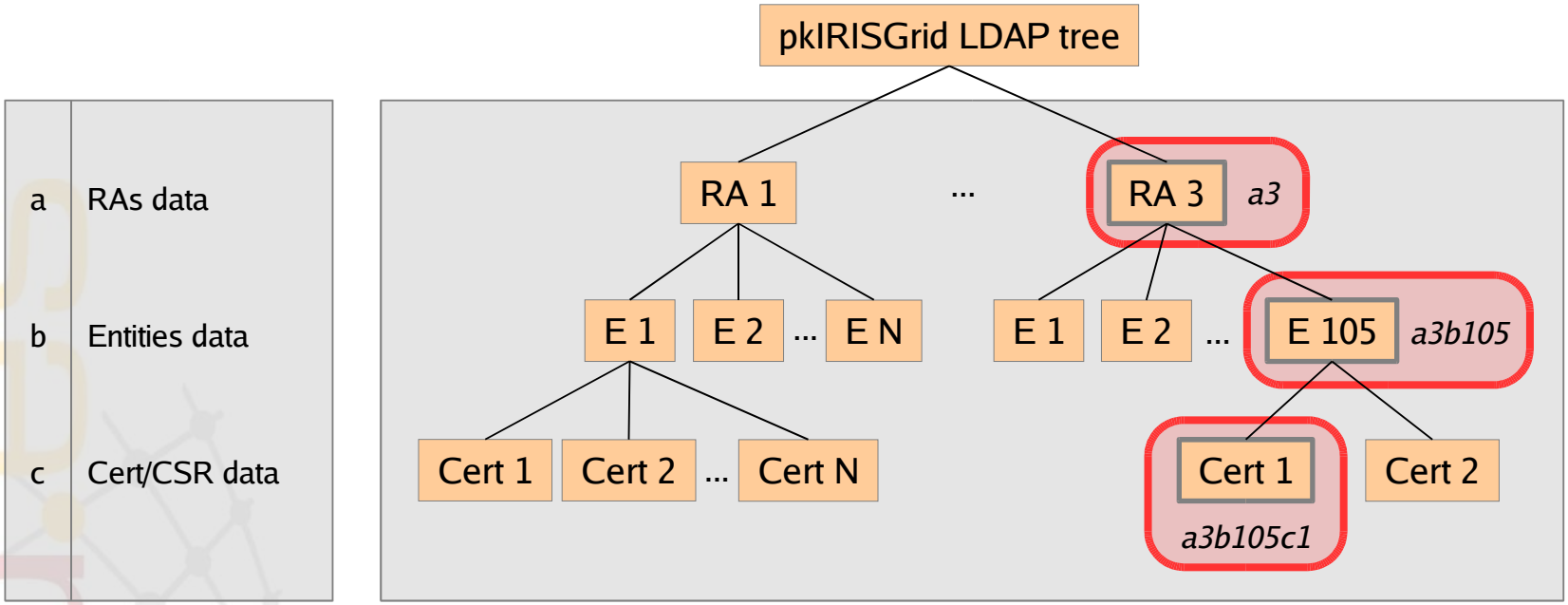


- pkirisgrid**RA**
  - pkirisgrid**ID** - *(COPA)*
  - pkirisgrid**RaName**
  - pkirisgrid**UsrCount**
- pkirisgrid**Usr**
  - pkirisgrid**ID** - *(COPA)*
  - cn
  - sn
  - telephoneNumber
  - mail

- pkirisgrid**Cert**
  - pkirisgrid**ID** - *(COPA)*
  - pkirisgrid**Trace**
  - pkirisgrid**Status**
  - pkirisgrid**Date**
  - pkirisgrid**Pin**
  - pkirisgrid**CSR**
  - pkirisgrid**CertType**
  - pkirisgrid**SubjectDN**
  - userCertificate

# pkIRISGrid
## COPA-based LDAP structure





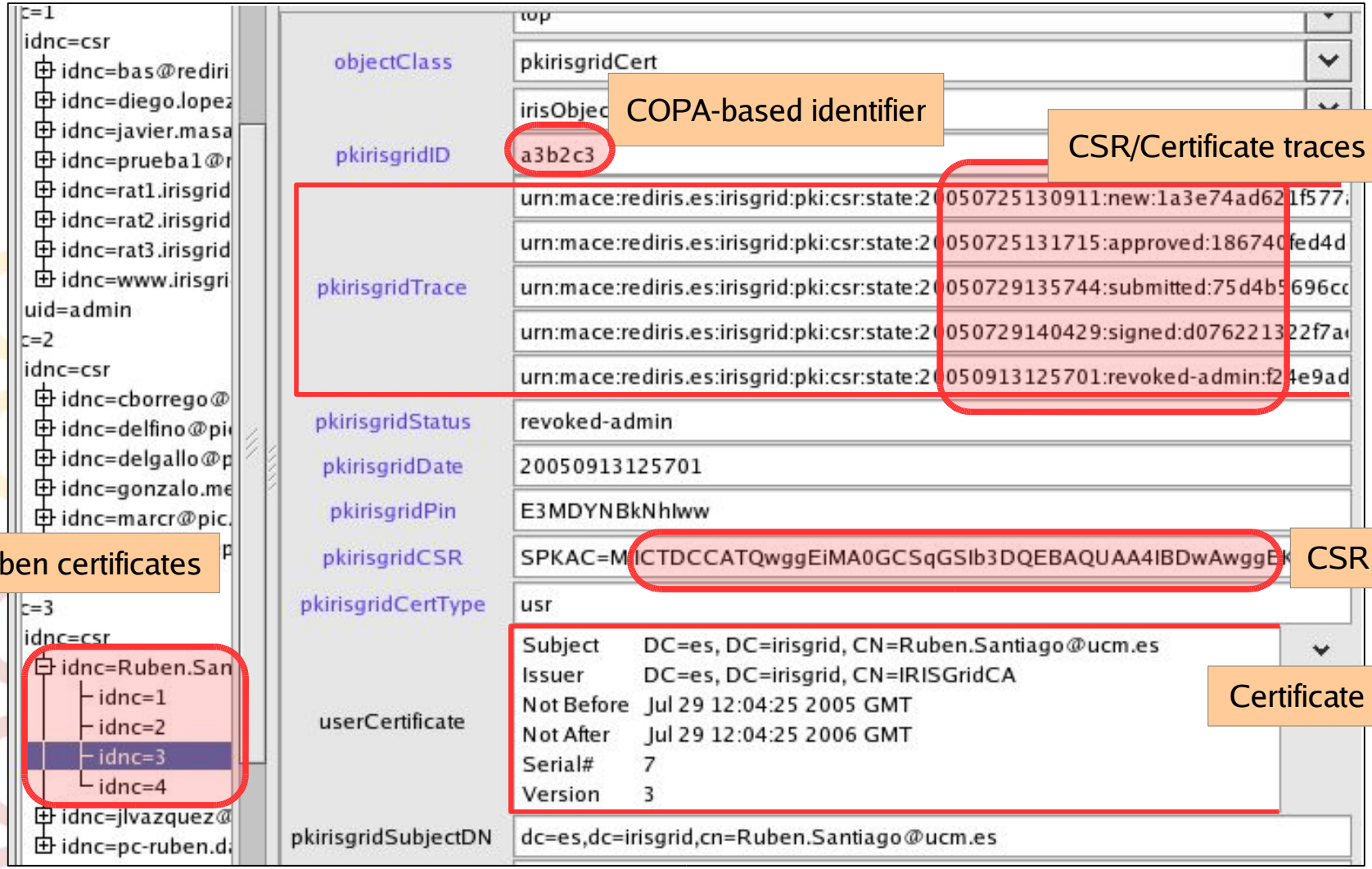

**a3** identifies RA 3

**a3b105** identifies RA 3, entity 105

**a3b105c1** identifies RA 3, entity 105, and certificate/CSR 1

# pkIRISGrid
## Certificate entry stored in LDAP





# pkIRISGrid CA
## Samples of file exchange between CA and RAs/Aux



- CSRs
  - XML file with CSRs sent to CA to issue certicates
  - LDIF file returned from CA
- CRRs
  - XML file with CRR data sent to CA
  - LDIF file returned from CA

# Sample files: XML file with CSRs
## sent to IRISGrid CA to issue certificates

```
<pkig>
<csrs>
<csr>
  <csr_header>
    <type_nav>SPKAC</type_nav>
    <type_ent>usr</type_ent>
    <dn>idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,...</dn>
    <serial>a2b2c1</serial>
    <trace>urn:mace:rediris.es:irisgrid:pki:csr:state:20050307171823:approved:2b4c41234b ... bde675d</trace>
  </csr_header>
<csr_data>
CN = antonio.robles@org.es
1.DC = irisgrid
0.DC = es
SPKAC=MIICTDCCATQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDow
     3R5/MPWuN0XW/05+hpgp3g5K1E7KUE8eIW+T/eiSwC3KPH..... W+NHCr8rn/FOpoyGw==
</csr_data>
  <csr_sig>c01e06d357edce49e ... 1bd687dae35cb520e332</csr_sig>
</csr>

<csr>
     ...
</csr>
</csrs>
<total_sig>7a29946e2c0a649ca ... 2f530122e2b39b2f3af9</total_sig>
</pkig>
```

CSR Header

CSR Data

# Sample files: LDIF file with certificates
## returned from the pkIRISGrid CA



```
# LDIF file. Upload it in pkIRISGrid CA
# User: antonio.robles@org.es
dn: idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,...
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed
-
replace: pkirisgridDate
pkirisgridDate: 20050230131552
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:20050230131552:signed:86fc84c4778e38 ... 46fc52198adc
-
replace: userCertificate;binary
userCertificate;binary::MIIFGDCCBACgAwIBAgIBFjANBgkqhkiG9w0BAQUFADBiMQsCQYDVQJAoGA1UE
 EAYKCZImiZPyLGQBGRMCZXMwHhcNMDUwMzMwMTExNTUxWhcNMDYwMzMwMTUxWjBpMRIwEAYD
 ......
 K4Q3AKwSVVxlykqycV059KJN2MDJWlpur2+/FwjkUyrXJwUG5kLPyPu7Jnxd4k54ifpQKJB7NVXu
 HkM549/gD9zVlkY9jAKCzKpkkXgF4ghRcMvNAS7OCs/Z4N8MNzSsOVsArD3XNXGcG+0l7Kop
```

LDIF entry 1

```
#User:  grid1.irisgrid.es
dn: idnc=1,idnc=grid1.irisgrid.es,idnc=csr,idnc=2,ou=ra,...
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed
.......
```

LDIF entry 2

# Sample files: XML file with CRRs
## data sent to pkIRISGrid CA

```
<pkig>
<crr_header>
  <crt_igID>a2b4c1</crt_igID>
  <crt_serial>22</crt_serial>
  <csr_dn>idnc=1,idnc=ww@ww.com,idnc=csr,...</csr_dn>
  <crr_ra>2</crr_ra>
  <crr_user>user</crr_user>
</crr_header>
<crr>
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 22 (0x16)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=es, DC=irisgrid, CN=IRISGridCA
        Validity
            Not Before: Mar 30 11:15:51 2005 GMT
            Not After : Mar 30 11:15:51 2006 GMT
        Subject: DC=es, DC=irisgrid, CN=www@www.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b8:ad:27:8e:03:95:b8:c6:18:0f:73:e2:df:b4:
                    6d:be:f5:2f:4c:b9:88:36:84:79:f5:93:6b:60:90:
                    ....
-----END CERTIFICATE-----
</crr>
<sig>61479b34d197f5d24 ... a22dbf0b9c4112557a49</sig>
</pkig>
```

CRR Header

Certificate

# LDIF file with revocation data
## Returned from CA

dn: idnc=1,idnc=ww@ww.com,idnc=csr,idnc=2,ou=ra,.....
changetype: modify
replace: **pkirisgridStatus**
pkirisgridStatus: **revoked-user**
-
replace: pkirisgridDate
pkirisgridDate: **20050304**142236
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:**20050304**142236:**revoked-user**:10e1608fbe...5f2ec57

# pkIRISGrid CA
## Certificate enrollment process (person) - I



- User
  - generate key pair with form provided at the pkIRISGrid web site
- Entry/CSR is stored in LDAP
- RA operator
  - Uses admin module to show all pending CSRs
  - Meet user to validate data and identity
- User
  - Shows ID card (with photo), CSR number, and introduces the PIN set when certificate was requested
- RA operator
  - Approves CSR
  - Uses admin module to export approved CSRs to CA

# pkIRISGrid CA
## Certificate enrollment process (person) - II



- CA operator
  - Receives CSRs and CRRs by mail, in XML format
  - Copy the file to an USB stick (aux1)
  - Starts CA laptop and attaches CA key USB stick
  - Execute CA software (ca, crr, crl, ...)
    - Software detects unauthorized data modifications
    - Signs, denies, revokes, generates CRL and produces LDIF file
  - Copy LDIF file to the USB stick (aux1)
  - Extracts USB sticks
  - Power off and stores laptop and CA key USB stick in vault

# pkIRISGrid CA
## Certificate enrollment process (person) - III



- CA operator
  - Carries USB stick (aux1) to a network access computer
  - Upload LDIF file to pkIRISGrid LDAP server
    - Update certificates, traces, revocations, CRLs, ...
    - Using ldapmodify command or another secure program
- Cron process
  - Finds entries modified today and
  - Sends mails with instruction to download certificates, ...

# pkIRISGrid CA: Future plans



- Update CP/CPS to obtain 1.0.0 version
  - A few weeks
- Finish the beta period of pkIRISGrid CA
  - Two months
- Become an EUGridPMA accredited CA
  - ASAP...
- Add new features to pkIRISGrid
  - Web-based CA software
  - New flat LDAP structure
  - Explore alternative interfaces

# Thanks you for your attention
## More information



- Example of RA for testing
  - Namespace:
    - irisgrid.es DC=es, DC=irisgrid, CN=name @ **irisgrid.es**
    - rediris.es DC=es, DC=irisgrid, CN=name @ **rediris.es**
    - rediris.com DC=es, DC=irisgrid, **O=RedIRIS**, CN=name @ **rediris.com**
  - URLs
    - https://rat1.irisgrid.es
    - https://rat1.irisgrid.es/admin/
- This presentation can be downloaded from:
  - http://www.irisgrid.es/coord/eugridpma/20050928-pkirisgrid.pdf
- Contact information
  - javier.masa @ rediris.es
- Questions?