Authorization & Authentication

Giuseppe La Rocca
INFN – Catania
giuseppe.larocca@ct.infn.it

EMBRACE-EGEE Tutorial

gLite Lightweight Middleware for Grid Computing

www.eu-egee.org

Information Society and Media

Overview

- Encryption
  - Symmetric algorithms
  - Asymmetric algorithms: PKI
- Certificates
  - Digital Signatures
  - X509 certificates
- Grid Security
  - Grid Security Infrastructure (GSI)
  - Proxy certificates
- Virtual Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS

Glossary

- Principal
  - An entity: a user, a program, or a machine
- Credentials
  - Some data providing a proof of identity
- Authentication
  - Verify the identity of a principal
- Authorization
  - Map an entity to some set of privileges
- Confidentiality
  - Encrypt the message so that only the recipient can understand it
- Integrity
  - Ensure that the message has not been altered in the transmission
- Non-repudiation
  - Impossibility of denying the authenticity of a digital signature

Authentication

- **Most grid infrastructures including the ones based on EGEE/LCG middleware use X.509 certificates.**

- **How does it work:**
  - **Each user, system or service must have a certificate that is used for authentication purposes**
  - **In order to identify and authenticate univocally each subject (user, system or service), the certificate must be signed by a trusted authority which task is to guarantee that the certificate belongs to the subject**
  - **These are the so called certification authorities (CAs) that:**
    - **Accept certificate requests and verify the subject identity**
    - **Signing the successfully verified certificates**
    - **Revoke certificates when needed**
    - **Issue lists of revoked certificates**

Authentication

- In the grid world one single CA usually covers a predefined *geographic region or administrative domain*:
  - Organization
  - Country
  - A set of countries
- A *common trust domain* for grid computing has been created to join the several existing certification authorities into a single authentication domain and thus enabling sharing of grid resources worldwide.
- The *International Grid Trust Federation* (IGTF) has been created to coordinate and manage this trust domain.
- IGTF is divided in three Policy Management Authorities (PMAs) covering the Asia Pacific, Europe and Americas.

International Grid Trust Federation

(Working to Establish Worldwide Trust for Grids)

www.gridpma.org

International Grid Trust Federation

Asia Pacific PMA

AIST Japan
APAC Australia
ASGCC Taiwan
SDG China
IHEP China
KISTI Korea
Naregi Japan
BMG Singapore
CMSD India
HKU Hong Kong
NCHC Taiwan
Osaka U. Japan
USM Malaysia

eugridpma

NorduGrid Nordic countries
PolishGrid Poland
Russian Datagrid Russia
SlovakGrid Slovakia
DataGrid-ES Spain
UK e-Science United Kingdom
BelnetGrid Belgium
Grid-PK Pakistan
FNAL Grid USA
GridCanada Canada
DOEGrids USA
ArmeSFo Armenia
IUCC Israel
ASCCG Taiwan
SeeGrid Europe
RMKI Hungary
SWITCH Switzerland
DFN Germany
RDIG Russia

LIP CA Portugal
CERN CA Switzerland
ArmeSFO Armenia
CNRS Grid France
CyGrid Cyprus
CESNET Czech
DutchGrid Netherlands
GermanGrid Germany
HellasGrid Greece
GridIreland Ireland
INFN CA Italy
Belnet Belgium
Grid-PK Pakistan
SIGNET Slovenia
EstonianGrid Estonia
AustrianGrid Austria
NIIF/HungarNet Hungary
IHEP China
BalticGrid Europe
TR-Grid Turkey

Americas PMA

DOEGrids USA
GridCanada Canada
FNAL USA

EUgridPMA

Is a body to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources. As its main activity the EUGridPMA coordinates a Public Key Infrastructure (PKI) for use with Grid authentication middleware. The EUGridPMA itself does not provide identity assertions, but instead asserts that the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

TAGPMA

- The Americas PMA is a regional PMA created to cover the Americas area from Canada to the tip of Chile.
- The TAGPMA was created in 2005 and its membership and activities are still reduced
- The appearance of potential new CAs in LA supported by the EELA project have been welcomed by TAGPMA and will be a major catalyst for this charter
- This is a situation also welcomed by the EUgridPMA that has already too many members
- Members of the TAGPMA which operate a classic PKI based Authentication service, must operate the service under the Classic PKI Authentication Profile that is maintained by the EU Grid PMA
- The EELA CAs must join the TAGPMA now

- For more information see: http://www.tagpma.org/

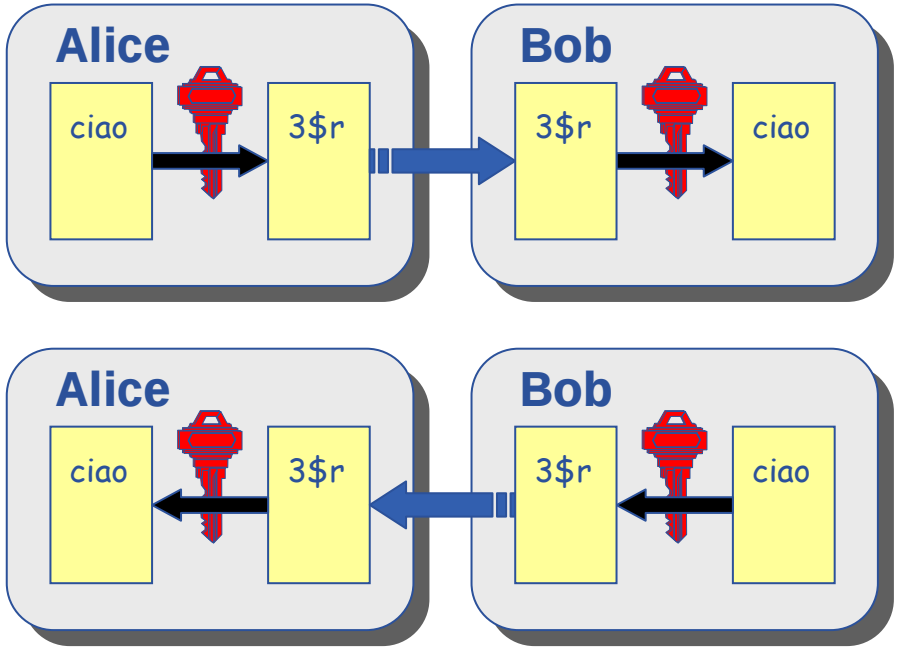
Cryptography

Cryptography

- Mathematical algorithms that provides important building blocks for the implementation of a security infrastructure
- Symbology
  - Plaintext: *M*
  - Cyphertext: *C*
  - Encryption with key K_1: $E_{K_1}(M) = C$
  - Decryption with key K_2: $D_{K_2}(C) = M$
- Algorithms
  - Symmetric: $K_1 = K_2$
  - Asymmetric: $K_1 \neq K_2$

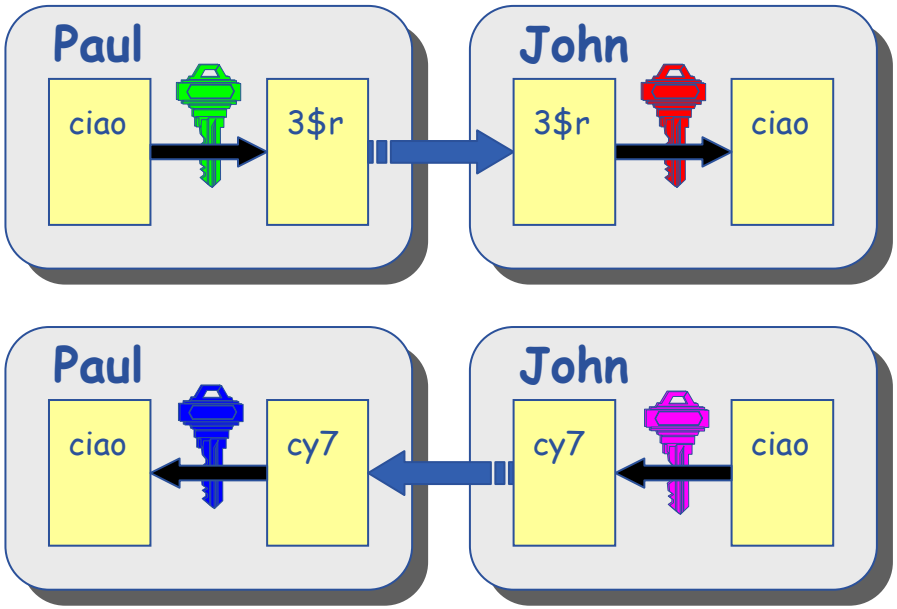
Symmetric Algorithms

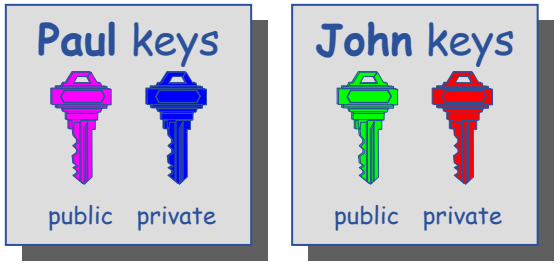
- The same key is used for encryption and decryption
- Advantages:
  - Fast
- Disadvantages:
  - how to distribute the keys?
  - the number of keys is $O(n^2)$
- Examples:
  - DES (56bit)
  - 3DES
  - Rijndael (AES)
  - Blowfish
  - Kerberos



Public Key Algorithms

- Every user has two keys: one *private* and one *public*:
  - it is *impossible* to derive the private key from the public one;
  - a message encrypted by one key can be decrypted only by the other one.
- No exchange of secrets is necessary
  - the sender cyphers using the *public* key of the receiver;
  - the receiver decrypts using his *private* key;
  - the number of keys is O(n).
- Examples:
  - **Diffie-Helmann** (1977)
  - **RSA** (1978)



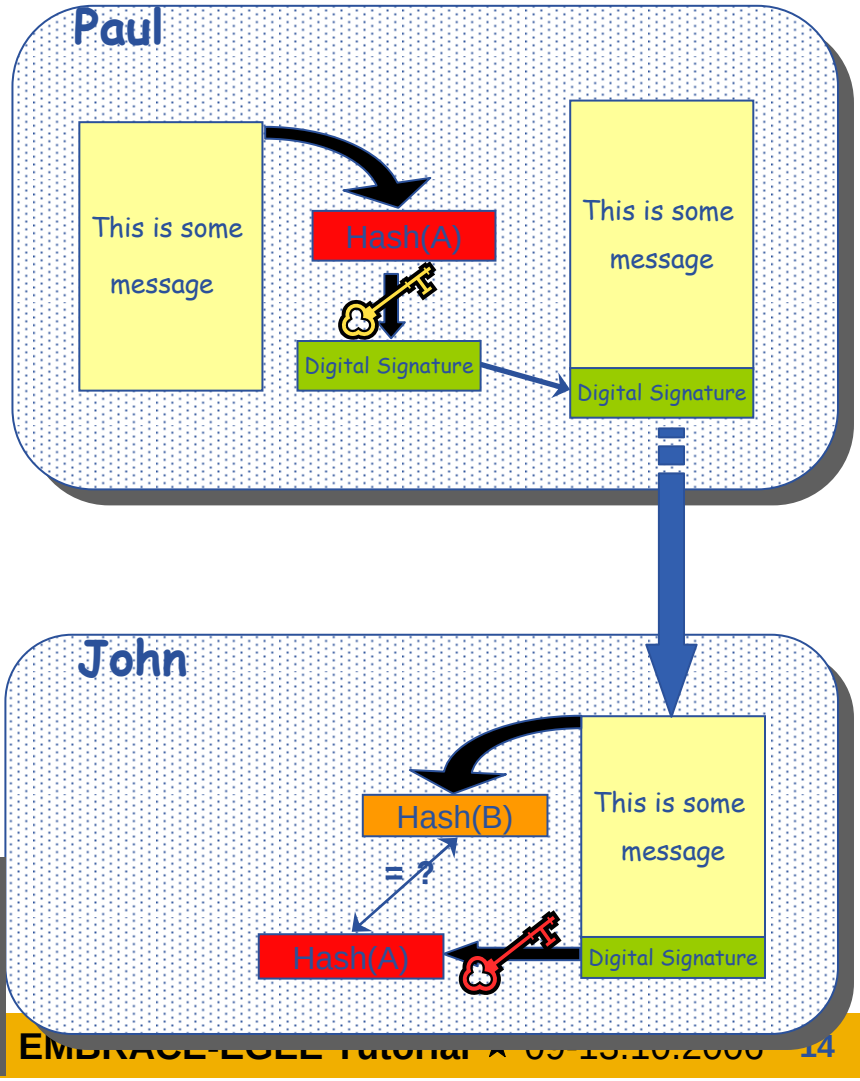


One-Way Hash function

- Functions (*H*) that given as input a variable-length message (*M*) produce as output a string of fixed length (*h*)
  - the length of *h* must be at least 128 bits (to avoid *birthday attacks*)
  1. given *M*, it **must be easy** to calculate $H(M) = h$
  2. given *h*, it **must be difficult** to calculate $M = H^{-1}(h)$
  3. given *M*, it **must be difficult** to find *M'* such that $H(M) = H(M')$
- **Examples:**
  - **SNEFRU**: hash of 128 or 256 bits;
  - **MD4/MD5**: hash of 128 bits;
  - **SHA** (Standard FIPS): hash of 160 bits.

Digital Signature

- Paul calculates the *hash* of the message (with a one-way hash function)
- Paul encrypts the hash using his *private* key: the encrypted hash is the *digital signature*.
- Paul sends the signed message to John.
- John calculates the hash of the message and *verifies* it with A, decyphered with Paul's *public* key.
- If hashes equal: message wasn't modified; Paul cannot repudiate it.



Digital Certificates

- Paul's digital signature is safe if:
  1. Paul's private key is not compromised
  2. John knows Paul's public key

- How can John be sure that Paul's public key is really Paul's public key and not someone else's?
  - A *third party* guarantees the correspondence between public key and owner's identity.
  - Both A and B must trust this third party

- Two models:
  - X.509: hierarchical organization;
  - PGP: "web of trust".

Certification Authority (CA)

The "third party" is called ***Certification Authority*** (CA).

- Issue **Digital Certificates** (containing public key and owner's identity) for users, programs and machines (signed by the CA)
- Check the identity and the personal data of the requestor
  - **Registration Authorities (RAs) do the actual validation**
- CA's periodically publish a list of compromised certificates
  - **Certificate Revocation Lists (CRL): contain all the revoked certificates.**
- CA certificates are **self-signed**

Revocation Lists v1

```
Certificate Revocation List (CRL):
        Version 1 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
        Last Update: Jan 24 15:04:47 2006 GMT
        Next Update: Feb 23 15:04:47 2006 GMT
Revoked Certificates:
    Serial Number: 1C
        Revocation Date: Jan  9 07:45:33 2002 GMT
    Serial Number: 1D
        Revocation Date: Jan  9 08:52:59 2002 GMT
...
    Serial Number: 0305
        Revocation Date: Dec  1 20:49:15 2005 GMT
    Signature Algorithm: sha1WithRSAEncryption
        32:d5:54:1e:4b:6b:35:d4:95:5b:5e:95:7f:38:73:32:24:a1:
        93:f6:91:98:bf:87:90:0e:cb:2a:f0:c0:0e:b3:6a:3a:9a:72:
        40:9a:c8:af:36:0e:5e:db:75:4a:6f:7e:83:5c:cd:01:41:91:
        4f:df:60:de:35:2a:a8:f5:85:dd:0d:b0:71:a2:ec:43:19:94:
        48:d8:ba:f5:46:65:ea:a9:1f:d2:d1:61:75:98:ef:e1:26:82:
        7d:8a:5e:9f:f4:8b:41:43:63:41:a6:57:cc:14:74:af:57:5a:
        67:4b:93:d3:e6:9c:76:5d:df:5e:99:37:6a:4d:b6:f0:5c:5d:
        e3:c0:cb:5e:ab:8f:ec:c0:01:d4:96:6f:9e:c7:9a:18:a3:24:
        46:a2:c4:54:30:e3:02:cb:89:cf:a7:3e:3f:39:a4:6b:ba:65:
        44:68:64:d6:1a:0d:08:eb:9a:41:34:31:2e:6e:4e:0e:7d:cc:
        d8:5c:50:c6:a7:96:df:40:ab:16:72:4c:c7:4e:96:51:8a:da:
        33:3f:db:a6:15:7e:53:dc:7f:86:09:94:30:cf:25:35:14:3d:
        12:36:20:e3:32:e9:b2:3d:ae:17:2f:78:89:32:2b:79:c5:32:
        d7:2e:61:43:d6:8a:f5:a3:63:3c:65:48:71:4c:20:76:c6:80:
        06:78:52:d0
```

The serial number of the revoked certificates

SHA1 must also be used to sign CRLs

Revocation Lists v2

```
Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /DC=cz/DC=cesnet-ca/CN=CESNET CA
    Last Update: Jan 27 22:51:32 2006 GMT
    Next Update: Feb  3 22:51:32 2006 GMT
    CRL extensions:
      X509v3 CRL Number:
        233
      X509v3 Authority Key Identifier:
        keyid:2F:6C:05:C3:51:26:AC:AF:39:9C:3E:38:35:DD:52:29:27:80:C5:F5

Revoked Certificates:
  Serial Number: 42B2FB6E
    Revocation Date: Jan 22 21:50:10 2006 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Superseded
  Serial Number: 42B2EB7B
    Revocation Date: Jul  4 12:21:58 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Unspecified
...
Signature Algorithm: sha1WithRSAEncryption
    b2:14:d3:b5:84:52:bf:ea:81:2d:96:a0:12:60:ac:ae:45:c1:
    42:12:05:57:09:1b:1a:14:83:41:b7:70:b0:26:f5:03:0f:8e:
    d4:99:18:d6:c5:f3:c2:77:6c:47:6e:c4:9c:21:9a:4c:01:02:
    9f:0a:50:cc:0b:e5:b0:7b:9d:4f:73:81:59:93:7f:56:d5:e7:
    99:ca:0f:a2:86:61:eb:5b:b6:44:b3:f9:61:01:5f:95:82:3f:
...
```

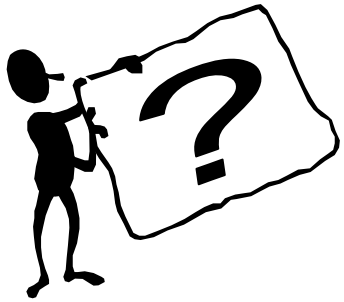
Extension containing the CRL number and CA key identifier

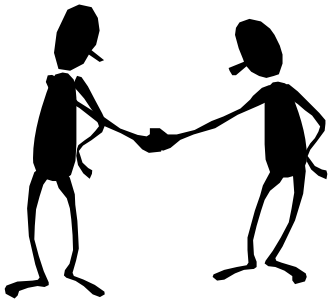
CRL entry extensions with the reason for revocation

X.509 certificates

CA Registration

- **How to obtain a certificate:**

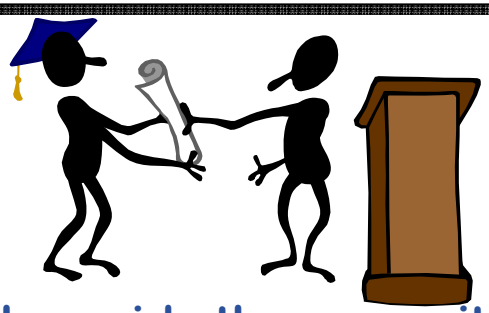




The users meets the RA (Registration Authority) that will verify the user's

The user

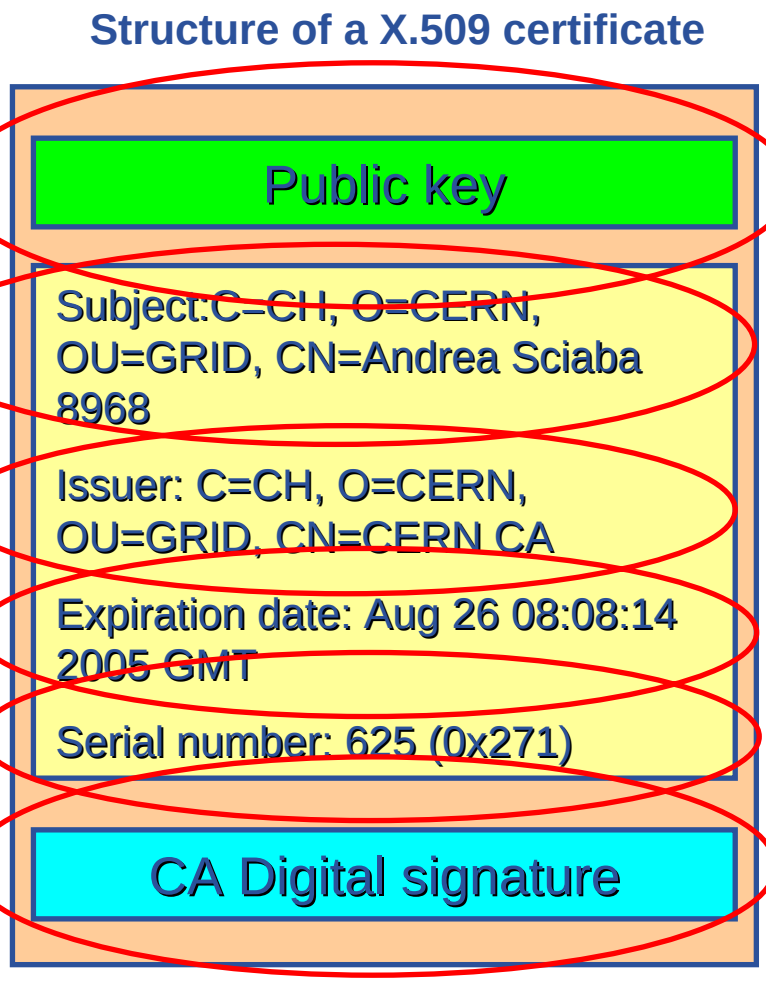
These steps are not needed to get a certificate from the GILDA CA



The RA will provide the user with a key to be used in the registration form to obtain a personal user's Certificate.

How does a X.509 certificate look like ?

- An X.509 Certificate contains:
  - owner's public key;
  - identity of the owner;
  - info on the CA;
  - time of validity;
  - Serial number;
  - digital signature of the CA



X.509 certificates - user

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 491 (0x1eb)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=NIKHEF, CN=NIKHEF medium-security certification auth
    Validity
      Not Before: Sep 29 14:26:09 2004 GMT
      Not After : Sep 29 14:26:09 2005 GMT
    Subject: O=dutchgrid, O=users, O=uva, OU=wins, CN=Breanndan O Nuallain
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:d4:b6:a1:9b:5f:fb:7e:0d:12:1d:0b:55:2c:6c:
            f8:ae:76:5b:43:96:d6:4a:7f:46:9a:9e:30:e6:85:
            fc:28:b1:77:d6:56:38:3b:6f:64:ad:46:ed:57:14:
            70:de:8b:1d:9e:76:7e:e5:af:57:e0:97:b8:ba:f6:
            ef:86:1d:b0:e5:5c:c1:13:40:67:4c:b6:d8:ef:50:
            01:09:3f:ee:5d:72:44:f8:30:fa:14:36:7d:b2:c4:
            06:69:bc:d9:81:60:ff:ae:21:88:b9:d9:5d:ed:41:
            04:ba:9f:eb:e7:7c:0b:5e:2f:f1:c3:29:56:8b:d6:
            79:75:0a:83:0e:3d:73:43:d5
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
      CA:FALSE
      X509v3 Key Usage:
      Digital Signature, Non Repudiation, Key Encipherment, Data
      Encipherment
      X509v3 CRL Distribution Points:
      URI:http://certificate.nikhef.nl/medium/cacrl.pem

      X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.1.10434.4.2.2.1.2.1

      X509v3 Authority Key Identifier:
      keyid:5B:05:3A:99:C6:D5:22:BD:FD:94:80:FC:11:A8:D0:F1:71:D6:4B:A4
      DirName:/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification
      auth
      serial:00

      X509v3 Subject Key Identifier:
      AD:4D:84:CB:4D:C8:AD:7A:E4:07:11:62:35:A0:97:FD:17:99:08:C7
      Netscape Cert Type:
      SSL Client, SSL Server, S/MIME
      Netscape CA Policy Url:
      http://certificate.nikhef.nl/medium/policy/
      Netscape Comment:
      Certificate issued under DutchGrid and NIKHEF medium-security policy
      version 2.1;limited liabilities apply, see
      http://certificate.nikhef.nl/medium/policy/ for details;Certificate Tag:
      8f2c35c8-d4b6a1
  Signature Algorithm: sha1WithRSAEncryption
    90:85:fc:87:16:5f:0d:3c:00:8f:6d:43:41:cb:d4:8f:cf:12:
    60:cd:94:25:ca:6d:33:df:a7:28:e1:b6:ff:69:31:f1:b6:f8:
    c9:ba:7b:07:90:cb:e0:7e:9d:98:f0:a2:54:9c:0e:2f:bd:b4:
    6e:d7:e9:fb:48:a9:82:9c:0e:44:37:a6:a8:67:39:c6:c0:8a:
    ac:70:2f:aa:1e:9f:28:bf:93:b2:8a:b2:81:bc:1c:95:6b:78:
    64:40:f0:de:17:ee:06:e6:51:10:9e:3d:98:94:1a:0b:2e:75:
    45:a7:89:7f:eb:13:11:9b:57:73:72:db:10:1b:26:cd:6e:67:
    a0:21:0d:da:b1:98:2b:be:a9:0a:27:ad:b8:60:06:44:44:58:
    3b:96:8e:af:2d:ba:e0:ee:b6:be:b3:0c:ad:65:4d:5e:21:2b:
    88:6d:c1:70:ab:24:7e:99:b3:95:ec:51:6e:8e:3b:b6:f0:32:
    90:50:87:51:a6:0f:2c:9e:57:53:99:57:09:05:33:94:77:1c:
    4c:91:6f:94:9c:d6:3b:85:0d:6a:5b:c2:d2:29:8f:5d:3d:3b:
    fb:a7:45:fd:6f:cb:e9:c5:95:54:cf:7b:84:53:08:ba:2f:7d:
    f5:50:6e:7b:2b:69:b2:92:c1:3b:54:33:b4:fc:06:2e:e3:2b:
    52:68:0a:1c
```

sha1 is OK

One year is OK

1024 bit pub key

These are violations of the profile critical is missing

Must point to the CRL URL

OID identifying the police under which this certificate was issued

SSL server is a strange thing in a user cert

X.509 certificates - user

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 397 (0x18d)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=PL, O=GRID, CN=Polish Grid CA
    Validity
      Not Before: Dec 20 15:47:38 2004 GMT
      Not After : Dec 20 15:47:38 2005 GMT
    Subject: C=PL, O=GRID, O=ICM, CN=Juliusz Gajewski
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:d1:30:fe:f7:af:0a:88:e7:84:96:7b:22:c6:2a:
          b4:3e:a7:f5:92:28:50:3c:ae:94:50:12:d7:ff:ef:
          29:ba:86:7f:a8:e8:27:d5:c0:7a:43:51:0f:97:12:
          59:1a:e7:70:2f:0e:34:bc:8b:11:dd:fc:3b:2e:6a:
          64:91:e6:93:73:95:fa:b1:7c:8c:11:9d:6a:16:58:
          80:36:4b:90:1c:2f:e5:de:23:4b:2b:30:6b:ba:4c:
          18:ce:33:c3:10:0f:ab:31:c7:04:90:bb:77:95:75:
          db:cf:4a:1f:6d:12:fc:18:5b:94:c0:b3:09:ac:0e:
          ae:f4:b8:93:24:bd:78:c6:cd
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
      CA:FALSE
      X509v3 Subject Key Identifier:
      14:6E:85:2F:89:91:41:32:E5:47:45:E4:91:17:CB:9A:E9:DC:76:D9
      X509v3 Authority Key Identifier:
      keyid:3C:2A:A1:84:45:6E:6F:94:F6:47:62:48:01:C1:B7:83:8F:CD:10:3D
      DirName:/C=PL/O=GRID/CN=Polish Grid CA
      serial:00
      X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment, Data
      Encipherment
      Netscape Cert Type:
      SSL Client, S/MIME, Object Signing
      X509v3 Issuer Alternative Name:
      email:plgrid-ca@man.poznan.pl
      X509v3 CRL Distribution Points:
      URI:http://www.man.poznan.pl/plgrid-ca/crl.pem

      Netscape Revocation Url:
      http://www.man.poznan.pl/plgrid-ca/crl.pem
      Netscape CA Policy Url:
      http://www.man.poznan.pl/plgrid-ca/ca-policy.html
      Netscape Comment:
      Certificate issued by Polish Grid CA
      Netscape Base Url:
      http://www.man.poznan.pl/plgrid-ca
  Signature Algorithm: md5WithRSAEncryption
    08:71:a6:fd:66:e1:42:4e:06:d6:bc:8b:31:be:fc:a2:6b:40:
    ea:62:24:29:06:12:35:60:24:f3:b0:7e:d0:81:e5:71:17:33:
    25:39:e3:55:26:32:f2:c1:46:93:c1:58:1a:b9:35:7f:ab:61:
    da:81:9f:ec:40:40:42:e1:f4:f7:0e:1b:5b:23:b1:fb:f4:bb:
    f1:08:22:74:97:51:28:23:86:75:bb:86:08:74:13:32:5e:e7:
    6e:cb:a3:c8:c3:74:f4:c3:ba:57:0b:d5:30:0b:ac:5f:c6:13:
    58:97:98:a4:cb:ca:a8:86:b0:94:18:8a:3b:af:0f:1a:52:9a:
    51:bc:07:6e:40:12:62:e4:d8:ad:c4:3b:4d:d2:e4:71:21:1f:
    59:63:81:95:10:8e:73:8c:85:b4:63:2a:8f:12:7b:ec:ea:f7:
    14:a5:51:ad:3f:2f:43:d3:33:40:81:66:fe:63:e3:31:e5:e8:
    f6:bb:54:ef:79:83:56:e8:5c:ae:6d:70:ef:1f:f2:17:ac:cc:
    0f:bb:08:57:ab:ac:1d:0c:d3:6b:22:af:44:2e:a4:ef:87:89:
    f8:fa:7c:7e:33:c7:ca:29:64:f0:74:e7:50:2f:91:66:2c:e1:
    da:32:c4:ee:a1:79:8c:91:f8:9d:0e:d5:5a:0c:19:a3:c8:16:
    f5:2b:15:46
```

VIOLATION must be SHA1

Critical is OK

Critical is OK

Email inside certificate
Take care with SPAM and privacy

VIOLATION THE OID IS MISSING

X.509 certificates - user

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 567 (0x237)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=FR, O=CNRS, CN=GRID-FR
    Validity
      Not Before: Dec 13 13:46:36 2005 GMT
      Not After : Dec 13 13:46:36 2006 GMT
    Subject: O=GRID-FR, C=BR, O=UFRJ, OU=IF, CN=Pedro Henrique Rausch
      Bello
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:bf:39:7f:79:b1:f2:fe:69:5f:85:85:64:c6:db:
          8c:61:90:cd:7a:84:53:14:a6:27:56:3d:d2:b5:e9:
          c8:6c:56:ce:c5:86:a5:66:98:ba:61:89:8f:aa:b4:
          8a:5a:f3:a5:c5:a2:8d:f3:7e:05:68:12:e3:d4:37:
          db:39:df:9d:63:42:82:20:83:ac:d3:a4:8c:07:cd:
          8e:de:01:4a:20:c7:a0:c2:d0:e4:95:c7:c0:18:35:
          53:39:88:01:a6:5e:1c:51:20:d8:c5:ac:42:c9:ed:
          b6:95:8c:db:3e:74:c4:e0:d0:2f:10:82:25:e3:fe:
          f6:27:c8:e8:5d:78:09:84:be:1b:7c:8f:80:a7:b9:
          34:4c:3d:9f:ba:7e:b8:a2:42:a0:2a:49:0d:2e:d7:
          a7:00:07:95:01:34:69:5b:82:b9:c2:82:59:18:ef:
          22:d7:3c:18:8f:2e:ef:70:68:6c:b1:2e:a9:f7:be:
          fb:ef:a1:f0:63:5d:f0:69:11:c6:6b:c3:cd:af:02:
          f5:30:f8:3b:f6:98:f8:d2:42:ed:64:dd:c6:8b:bb:
          7a:d7:3e:ca:de:0c:cf:6f:64:19:ae:5f:f3:e2:c7:
          de:dd:89:36:f7:14:9e:05:74:cb:99:49:81:b4:3e:
          26:51:0b:bc:74:ab:1a:d0:dd:f0:f0:ea:fc:d6:45:
          a8:d3
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
      CA:FALSE
      Netscape Cert Type:
      SSL Client, S/MIME, Object Signing
      X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment, Data
      Encipherment, Key Agreement
      Netscape Comment:
      Certificat GRID-FR. Pour toute information se reporter à
      http://igc.services.cnrs.fr/GRID-FR/
      X509v3 Subject Key Identifier:
      B9:91:66:35:91:15:51:84:2D:ED:87:31:0A:5A:24:4A:00:74:9D:E8
      X509v3 Authority Key Identifier:
      keyid:77:49:79:C1:F6:BB:92:F0:EC:08:C3:EE:D1:9C:B0:77:10:8C:93:2F
      DirName:/C=FR/O=CNRS/CN=CNRS-Projets
      serial:0C

      X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.1.10813.1.1.8.1.0

      X509v3 Subject Alternative Name:
      email:rausch@if.ufrj.br
      X509v3 CRL Distribution Points:
      URI:http://crls.services.cnrs.fr/GRID-FR/getder.crl

      1.3.6.1.4.1.7650.1:
        unicoreClient
  Signature Algorithm: sha1WithRSAEncryption
    6b:6b:da:49:82:7d:77:1c:9b:e1:ef:c0:90:c2:9e:7e:ca:b9:
    40:62:bf:2c:fa:10:f4:ea:94:d4:90:09:69:9d:2b:91:94:3a:
    c4:be:5b:5b:56:55:0d:f9:8c:4d:a1:f3:aa:61:29:e9:f1:45:
    ed:de:32:05:f3:70:20:4d:2d:ee:04:50:5a:32:56:b7:f1:23:
    2c:a0:d6:41:10:58:5c:28:fc:df:95:15:44:76:80:5d:4d:9a:
    ae:20:6c:d1:2c:df:70:1c:bb:ed:c1:f7:1c:f3:8c:18:d6:bb:
    ef:6b:60:63:ab:89:9d:62:99:19:9d:84:be:f2:d7:34:c3:3d:
    de:22:80:12:71:c0:bb:3c:f8:9a:8a:fd:5b:c2:6b:b9:7f:3f:
    8a:ed:5d:e4:d9:c5:02:04:67:53:2d:e6:ff:df:20:e4:80:5b:
    bc:d2:55:0e:d4:98:c8:5e:02:0f:bc:c3:87:1c:94:fc:c0:51:
    a1:a2:01:0f:4e:62:86:1f:9d:25:57:ee:82:1b:53:d3:13:a7:
    05:98:04:85:05:1f:a1:69:96:07:4a:1f:fb:90:24:55:6c:36:
    fb:f5:be:78:a4:23:98:50:85:b4:c4:de:51:d3:54:ca:2f:19:
    60:89:8f:8b:14:e7:8e:50:6a:52:64:be:53:d7:63:d7:97:b8:
    0b:fc:78:85
```

Key can be > 1024

Email inside certificate
Take care with SPAM and privacy

X.509 certificates - host

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 62 (0x3e)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=PT, O=LIPCA, CN=LIP Certification Authority
    Validity
      Not Before: Nov 23 11:23:53 2005 GMT
      Not After : Nov 23 11:23:53 2006 GMT
    Subject: C=PT, O=LIPCA, O=LIP, OU=Lisboa, CN=ce01.lip.pt
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:de:90:2a:43:49:e6:a3:88:df:a6:8b:6b:b8:31:
          7d:66:17:b4:1a:37:6e:5c:a5:e8:ea:61:67:f3:ff:
          67:11:5e:4f:ff:26:f1:ee:b4:34:cc:d7:07:59:e7:
          1b:ab:cc:7d:ec:23:4c:48:0c:86:61:4f:8f:11:09:
          c8:4c:6b:73:e1:a9:fa:36:83:6f:30:b4:41:e1:2f:
          1c:35:97:7f:44:0e:d0:87:8a:f7:75:f6:ce:bc:8e:
          1c:ba:c1:1c:ec:dc:0e:64:53:d2:84:23:18:f2:b1:
          5f:b7:54:d2:aa:7e:9a:af:cc:0a:7f:1e:76:d9:c8:
          99:3c:d7:b2:70:d3:ac:d4:b1
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      Netscape Cert Type:
        SSL Server
      X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment, Data
      Encipherment
      Netscape Comment:
        LIP Certification Authority Server Signed Certificate
      X509v3 Subject Key Identifier:
        F6:FF:63:E5:C5:3D:CA:F5:98:A8:A9:E6:7E:22:B3:5F:82:6F:65:80
      X509v3 Authority Key Identifier:
        keyid:42:AE:6E:F7:86:1E:9E:E8:68:EF:CF:79:53:38:62:4E:00:F2:42:EC
        DirName:/C=PT/O=LIPCA/CN=LIP Certification Authority
        serial:00
```

Here it makes sense

```
      X509v3 Subject Alternative Name:
        DNS:ce01.lip.pt
      X509v3 Issuer Alternative Name:
        email:ca@lip.pt
      Netscape CA Revocation Url:
        http://ca.lip.pt/crl/crl.pem
      Netscape CA Policy Url:
        http://ca.lip.pt/policy
      X509v3 CRL Distribution Points:
        URI:http://ca.lip.pt/crl/crl.pem

      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.9846.10.1.1.4.1

Signature Algorithm: sha1WithRSAEncryption
    76:01:71:f4:4e:13:88:c7:8a:f9:d7:27:f6:ba:09:5a:a3:d9:
    01:b6:8a:76:da:5a:9a:06:c2:23:84:b6:07:d0:5a:ab:b3:db:
    ba:f9:17:91:58:4e:48:c6:6b:5d:4b:fd:31:2d:89:09:20:31:
    f7:fa:7a:4f:73:de:3c:4c:2c:89:90:36:5f:36:32:e6:16:3f:
    20:80:96:64:c3:e2:22:7f:42:fc:95:0c:49:33:ba:b9:eb:ec:
    df:b9:a4:0d:ae:82:e4:66:44:78:fd:9b:d8:a4:65:9c:55:ff:
    40:01:d9:ee:95:d0:95:7c:86:3e:77:12:8e:2f:90:fb:f6:e1:
    41:1e:5c:b5:ee:20:8e:87:41:71:46:ea:23:bf:e7:27:9a:cb:
    81:98:87:73:5b:1f:cc:98:79:d0:fb:ca:62:7e:6d:ee:be:77:
    d5:dc:18:87:f6:c2:eb:3f:63:71:d2:aa:3f:08:ac:d7:05:85:
    33:8d:7e:35:f3:10:41:fe:9a:e9:65:14:10:ad:ed:c5:59:4f:
    7d:5b:c7:f7:f3:67:e7:26:75:22:4d:3a:43:e5:c4:0f:28:4c:
    56:b1:e4:f0:20:27:7b:00:e4:f0:bd:96:04:be:f3:c1:1e:fc:
    aa:a4:3e:92:38:a1:24:96:ba:2d:38:7d:72:6f:fe:97:fc:51:
    a7:3f:34:1e
```

Hostname must be encoded in a subject alternative name extension of type DNS

X.509 certificates - host

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 72 (0x48)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=PT, O=LIPCA, CN=LIP Certification Authority
    Validity
      Not Before: Jan 17 16:44:53 2006 GMT
      Not After : Jan 17 16:44:53 2007 GMT
    Subject: C=PT, O=LIPCA, O=LIP, OU=Lisboa, CN=host/voms.lip.pt
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:be:09:4a:bb:52:77:92:e5:ae:8b:b0:a4:ff:8b:
          1f:1a:91:fa:bc:04:13:9f:a5:1e:cd:16:21:12:60:
          b6:59:42:75:cc:f3:27:d4:5b:5d:8f:58:5d:c5:14:
          e3:b5:61:ae:c4:16:a1:bf:35:ff:78:10:bb:3b:92:
          bf:fa:1e:6a:d6:31:bb:c7:0d:f0:f8:17:7d:f7:07:
          b9:7b:7a:ba:d3:72:32:3a:05:cc:18:5e:e2:aa:b6:
          a2:db:89:61:03:b1:28:b7:5d:49:18:b8:5f:67:4d:
          e5:2c:19:e8:8c:a5:49:3e:91:20:7f:f1:65:9f:d5:
          be:4b:bb:5d:0d:5b:f0:f3:2b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      Netscape Cert Type:
        SSL Server
      X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment, Data
      Encipherment
      Netscape Comment:
        LIP Certification Authority Server Signed Certificate
      X509v3 Subject Key Identifier:
        8C:99:8A:E5:85:8B:CF:B3:EE:8C:98:CE:85:9F:F0:57:16:8B:36:DA
      X509v3 Authority Key Identifier:
        keyid:42:AE:6E:F7:86:1E:9E:E8:68:EF:CF:79:53:38:62:4E:00:F2:42:EC
        DirName:/C=PT/O=LIPCA/CN=LIP Certification Authority
        serial:00
```

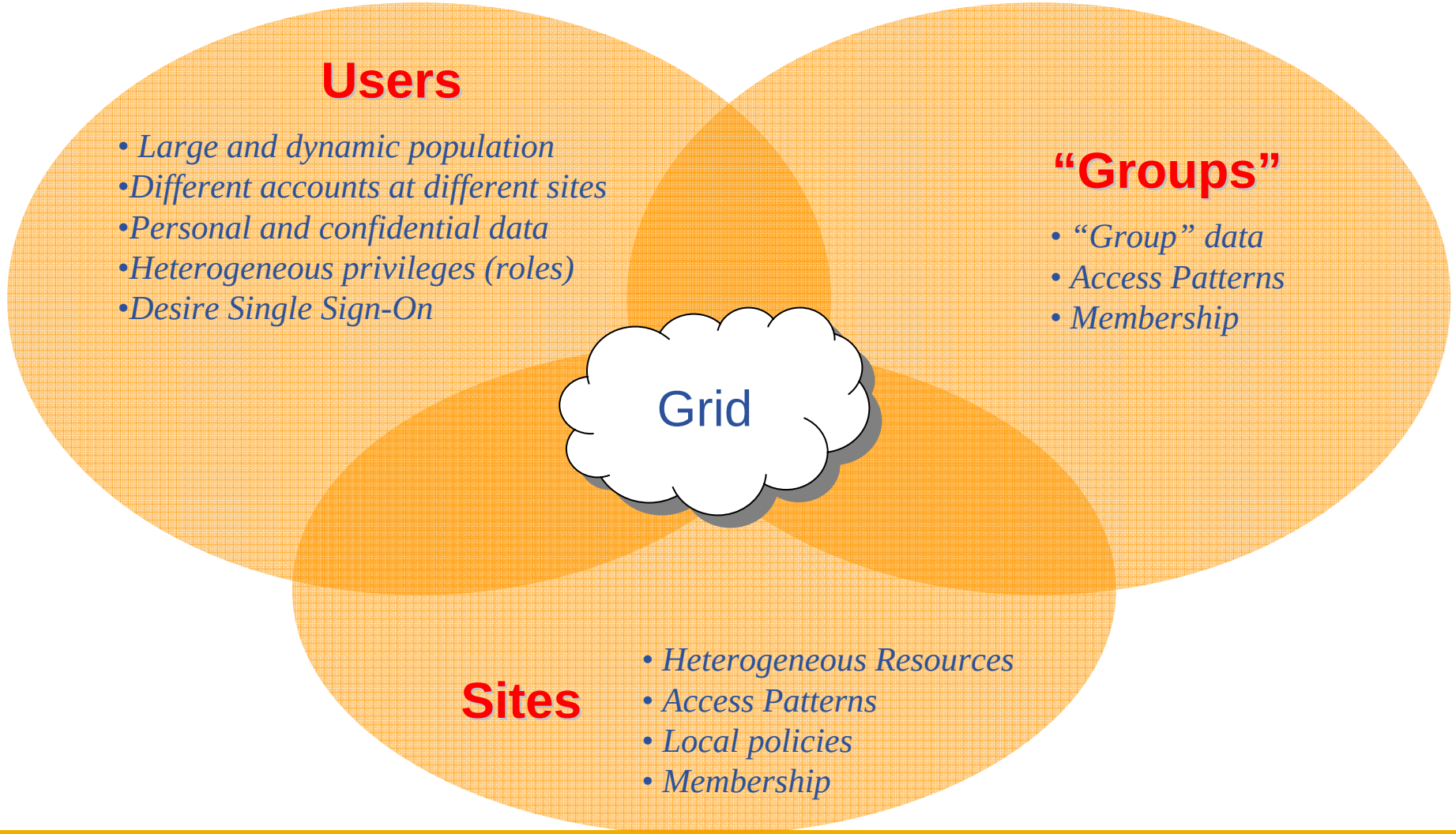
A different form of specifying a hostname

```
      X509v3 Subject Alternative Name:
        DNS:voms.lip.pt
      X509v3 Issuer Alternative Name:
        email:ca@lip.pt
      Netscape CA Revocation Url:
        http://ca.lip.pt/crl/crl.pem
      Netscape CA Policy Url:
        http://ca.lip.pt/policy
      X509v3 CRL Distribution Points:
        URI:http://ca.lip.pt/crl/crl.pem

      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.9846.10.1.1.4.1

Signature Algorithm: sha1WithRSAEncryption
    91:0c:70:99:11:72:a9:82:58:e7:9d:cf:78:e5:cd:e4:e5:91:
    b9:41:8d:d5:9e:21:c4:1e:29:4b:e6:e5:d5:b2:97:e6:d9:27:
    5b:55:21:42:96:d6:8b:da:39:fa:96:ab:d8:2d:c0:49:0f:82:
    a3:b5:bf:3d:27:a5:4b:d6:d0:84:52:ba:4c:b8:b9:6d:70:bc:
    35:19:53:5b:ed:21:9b:bc:19:36:bb:00:ca:8e:cb:49:fc:6f:
    a1:7d:13:02:55:37:96:a6:94:a6:33:93:d6:2c:bc:35:d8:07:
    dd:7c:f8:9c:6d:c8:af:6f:56:7a:fc:1d:0a:0f:35:41:51:b1:
    fb:a1:52:f0:ab:98:f6:94:ea:4b:2e:6f:45:7f:e1:22:b3:e5:
    56:ca:6f:73:8f:3f:c8:1f:65:3b:75:26:e0:a9:27:4b:60:21:
    3f:58:35:ce:86:e0:93:9e:21:0d:ee:33:d1:75:e6:79:6a:4a:
    49:45:80:b0:53:01:d1:8e:28:8e:a7:80:78:b1:7b:b9:a4:c9:
    eb:e8:9b:28:32:47:3d:68:9c:ab:81:99:27:e0:26:a7:d3:f8:
    a5:05:b2:2b:54:ba:d5:62:7d:37:d7:bd:61:4f:ed:3f:48:2f:
    16:65:3b:62:6c:1c:25:0f:2c:13:88:4a:86:f5:5b:5f:72:c9:
    80:34:21:ca
```

The scenario..



The Grid Security Infrastructure (GSI)

Based on X.509 PKI:

- every user/host/service has an X.509 certificate
- certific
  local s
- every
  authen
  1. Jo
  2. Pa
     ce
  3. Pa
  4. Jo
     his
  5. Jo
     Pa
  6. Pa
     the
  7. Paul compares the decrypted string with the original challenge
  8. If they match, Paul verified John's identity and John can not repudiate it.

VERY IMPORTANT

Private keys must be stored only:

in ***protected*** places

AND

in ***encrypted*** form

Delegation and Single Sign-On

- The GSI provides a delegation capability which reduces the number of times the user must enter his pass phrase.
- If a Grid computation requires that several Grid resources must be used, the need to re-enter the user's pass phrase can be avoided by creating a *proxy*.
- A proxy is a sort of new certificate.
  - The new certificate contains the *owner's identity*, modified slightly to indicate that it is a proxy.
  - The new certificate is *signed by the owner*, rather than a CA.
  - Proxies *have limited lifetimes*.

Certificate request… more details

- Identity Credential Formats: X.509 Certificate
- Egee/LCG recognizes a given set of CAs
  - https://lcg-registrar.cern.ch/pki_certificates.html
  - http://www.eugridpma.org/
- How do you request a certificate depends on your CA (EU Grid PMA)
- For GILDA, have a look at the Video Tutorials:
  - https://gilda.ct.infn.it/video/Certification/Allproxy.html (Flash)
  - https://gilda.ct.infn.it/video/Certification/AllCertproxy.ram (Real)

On the side: certificate management

- Import your certificate in your browser
  - If you received a *.pem* certificate you need to convert it to PKCS12
  - Use *openssl* command line (available in each EGEE/LCG UI)
    - `openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out my_cert.p12 -name 'My Name'`
- GILDA (and other VOs):
  - You receive already a PKCS12 certificate (can import it directly into the web browser)
  - For future use, you will need *usercert.pem* and *userkey.pem* in a directory ~/.globus on your UI
  - Export the PKCS12 cert to a local dir on UI and use again *openssl:*
    - `openssl pkcs12 -nocerts -in my_cert.p12 -out userkey.pem`
    - `openssl pkcs12 -clcerts -nokeys -in my_cert.p12 -out usercert.pem`

Virtual Organization, VOMS & MyProxy

Virtual Organizations

- VOs are basically groups of users that share common or similar interests and share the same resources.
- Authorization is based on the VO concept. Instead of authorizing users individually, site access is allowed on a VO basis enabling better scalability.
  - The site manager does not need to add individual users
  - The site manager authorizes entire VOs
  - The site manager can refuse specific certificate subject patterns
- The VO manager is responsible for allowing or denying access to the VO based on the VO policies.
- The possession of a certificate does not gives the right of access to any grid resources by itself.

Virtual Organizations

- At each site each user certificate is mapped into a unique local user account
  - This happens the first time the user accesses the resource
  - Local user accounts are taken from a pool assigned to the VO

- Two different types of VO management exist:
  - LDAP based VOs
    - This is the oldest method, it is based on an LDAP server that contains the list of VO members.
    - To authorize the VO the site manager maps the server URL into a pool of accounts, a local authorization file is rebuilt every few hours from the LDAP server
  - VOMS
    - The list of authorized persons together with their rights and roles in stored in a VOMS server
    - While obtaining a proxy grid certificate the VOMS server is contacted and it encodes the user VO name, rights and roles inside the proxy.
    - The grid resources check these extensions during the authorization phase and enforce them.

VOMS

- *Virtual Organization Membership Service* (VOMS) is a service that keeps track of the members of a VO and *grants users authorization* to access the resource at VO level.
  - **Its provides support for group membership and roles membership (e.g. administrator, sofware manager, student).**

- Each VO has its own server(s) containing groups membership, roles and information for each user.
- User contacts the server requesting his authorization info.
- The server sends the authorization info to the client.
- The client includes it in a proxy certificate.

FQAN

- **Fully Qualified Attribute Name (FQAN), is what VOMS uses to express membership and other authorization info**
- **Groups membership, roles and capabilities may be expressed in a format that bounds them together <group>/Role=[<role>][/Capability=<capability>]**

```
[larocca@glite-tutor larocca]$ voms-proxy-info -fqan
/gilda/Role=TrailersManager/Capability=NULL
```

- **FQAN are included in an Attribute Certificate (AC)**
- **Attribute Certificates are used to bind a set of attributes (like membership, roles, authorization info etc) with an identity**

LCAS & LCMAPS

- At resources level, authorization info are extracted from the proxy and processed by ***LCAS*** and ***LCMAPS***

- Local Centre Authorization Service (LCAS)
  - Checks if the user is authorized (currently using the grid-mapfile)
  - Checks if the user is banned at the site

- Local Credential Mapping Service (LCMAPS)
  - Maps grid credentials to local credentials (eg. UNIX uid/gid, AFS tokens, etc.)
  - Map also VOMS group and roles (full support of FQAN)

```
"/VO=cms/GROUP=/cms"                    .cms
"/VO=cms/GROUP=/cms/prod"               .cmsprod
"/VO=cms/GROUP=/cms/prod/ROLE=manager"  .cmsprodman
```

voms-proxy-init – example usage

Enabling Grids for E-sciencE

```
[larocca@glite-tutor:~]$ voms-proxy-init --voms gilda

Your identity: /C=IT/O=GILDA/OU=Personal
  Certificate/L=INFN Catania/CN=Giuseppe La
  Rocca/Email=giuseppe.larocca@ct.infn.it
Enter GRID pass phrase:
Your proxy is valid until Sat Feb  4 01:08:28 2006

Creating temporary proxy
  ..................................... Done
Contacting  voms.ct.infn.it:15001
  [/C=IT/O=GILDA/OU=Host/L=INFN
  Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.i
  nfn.it] "gilda" Done
Creating proxy .................................
  Done
Your proxy is valid until Sat Feb  4 01:08:38 2006
```

voms-proxy-info – example usage

Enabling Grids for E-sciencE

```
[larocca@glite-tutor:~]$ voms-proxy-info --all
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La
   Rocca/Email=giuseppe.larocca@ct.infn.it/CN=proxy
issuer    : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it
identity  : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.lar    ca@ct.infn.it
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u512
timeleft  : 11:55:52
=== VO gilda extension information ===
VO        : gilda
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=I   FN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it
issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
   Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it
attribute : /gilda/Role=NULL/Capability=NULL
timeleft  : 11:55:41
```

voms-proxy-init – common problems

- ```
  [larocca@glite-tutor larocca]$ voms-proxy-init --voms pippo
  VOMS Server for pippo not known!
  ```

  The specified vo nickname is not present in any of the configuration files.

- ```
  [larocca@glite-tutor larocca]$ voms-proxy-init --voms dteam
  Your identity: /C=IT/O=INFN/OU=Personal
  Certificate/L=INFN/CN=Giuseppe
  La Rocca/Email=giuseppe.larocca@ct.infn.it
  Enter GRID pass phrase for this identity:
  Creating temporary proxy
  ..................................... Done
  /C=CH/O=CERN/OU=GRID/CN=host/voms.cern.ch
  /C=CH/O=CERN/OU=GRID/CN=CERN CA
  Can't interpret AC!
  dteam: Unable to satisfy G/dteam Request!
  ```

  The user is not a member of the VO. Contact the VO manager to request membership.

voms-proxy-info – common problems

```
[larocca@glite-tutor larocca]$ voms-proxy-info
error = 5025
WARNING: Unable to verify signature!
subject   : /C=IT/O=INFN/OU=Personal
Certificate/L=INFN/CN=Giuseppe
La Rocca/Email=giuseppe.larocca@ct.infn.it/CN=proxy
issuer    : /C=IT/O=INFN/OU=Personal
Certificate/L=INFN/CN=Giuseppe La
Rocca/Email=giuseppe.larocca@ct.infn.it
identity  : /C=IT/O=INFN/OU=Personal
Certificate/L=INFN/CN=Giuseppe La
Rocca/Email=giuseppe.larocc@ct.infn.it
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u501
timeleft  : 11:07:16
```

A problem occurred verifiyng the AC signature. The host certificate of the VOMS server is not present in the $X509_VOMS_DIR (default /etc/grid-security/vomsdir) directory.

Groups

- The number of users of a VO can be very high:
  - E.g. the experiment ATLAS has 2000 member

- Make VO manageable by organizing users in groups:

  Examples:
  - VO GILDA
    - Catania's group
      - *INFN*
        - Group Barbera
      - *University*
    - Padua's group
    - …

- Groups can have a hierarchical structure, undefinitely deep

Roles

- With roles it is possible to distinguish a user from others in his group:
  - Software manager
  - VO-Administrator
- Difference between roles and groups:
  - Roles have no hierarchical structure – there is no sub-role
  - Roles are not used in 'normal operation'
    - They are not added to the proxy by default when running *voms-proxy-init*
- Example:
  - User Emidio has the following membership
    - VO=gilda, Group=tutors, Role=SoftwareManager
  - During normal operation the role is not taken into account, e.g. Emidio can work as a normal user
  - For special things he can obtain the role "Software Manager"

Requesting group/role membership

- Any group membership is automatically added when performing voms-proxy-init
- Default group is /<vo-name>, if not differently specified it's the 1st group inserted in attributes.

- User can specify a different order for groups

```
voms-proxy-init --voms gilda:/gilda/
```

- Role membership has to be requested explicitly

```
voms-proxy-init --voms gilda:/Role=TrailersManager
```

Long term proxy

- Proxy has limited lifetime (default is 12 h)
  - Bad idea to have longer proxy
- However, a grid task might need to use a proxy for a much longer time
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days

- myproxy server:
  - Allows to create and store a long term proxy certificate:
  - myproxy-init -s <host_name>
    - -s: <host_name> specifies the hostname of the myproxy server
  - myproxy-info
    - Get information about the long living proxy
  - myproxy-get-delegation
    - Get a new proxy from the MyProxy server
  - myproxy-destroy

VOMS and MyProxy

- MyProxy supports just plain proxies **without** voms extension
- To allow storing of voms ext., myproxy client has been modified

```
myproxy-init --voms gilda:/Role=VO-Admin
```

- Proxies then retrieved with **myproxy-get-delegation** will have the requested voms extension but there's a limitation, due to voms extensions lifetime: *tipically it's limited, and it's not renewed when performing myproxy-get-delegation!!*

- The "modified" client is available on all of GILDA's UI.

voms extension on a delegated proxy


```
[ui-test] /home/giorgio > myproxy-get-delegation -s grid001.ct.infn.it
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in /tmp/x509up_u500

[ui-test] /home/giorgio > voms-proxy-info --all
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy/CN=proxy
issuer    : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy
identity  : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy
type      : unknown
strength  : 512 bits
path      : /tmp/x509up_u500
timeleft  : 12:00:09
=== VO gilda extension information ===
VO        : gilda
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
   Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it
attribute : /gilda/Role=NULL/Capability=NULL
attribute : /gilda/tutors/Role=NULL/Capability=NULL
timeleft  : 0:00:00
```

Voms extension expired…

References

- VOMS suite : user and installation guide
  - http://infnforge.cnaf.infn.it/voms/software.pdf
- MyProxy user's guide
  - http://grid.ncsa.uiuc.edu/myproxy/credmgmt.html
- VOMS with MyProxy, how to
  - http://egee-na4.ct.infn.it/genapps/wiki/index.php/VomsMyProxy
- VOMS
  - Available at http://infnforge.cnaf.infn.it/voms/
  - Alfieri, Cecchini, Ciaschini, Spataro, dell'Agnello, Fronher, Lorentey, From gridmap-file to VOMS: managing Authorization in a Grid environment
  - Vincenzo Ciaschini, A VOMS Attribute Certificate Profile for Authorization

Questions...