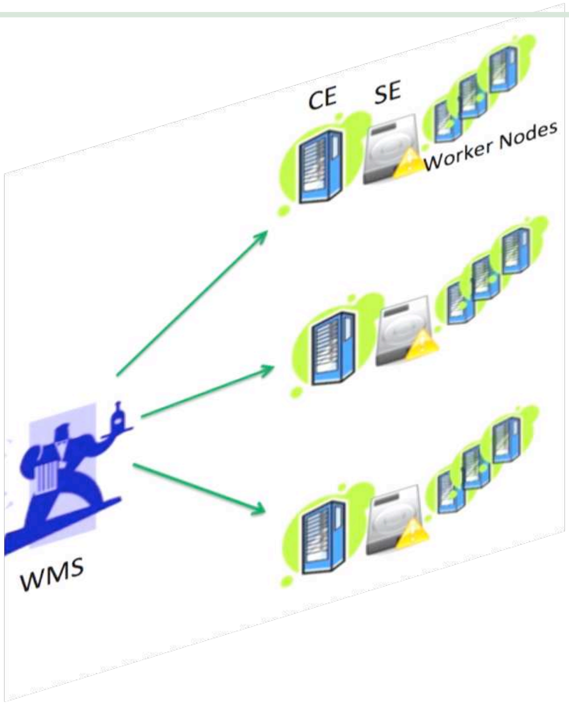
Grid Certificate I
Security

SURFsara – Online Grid Computing Course

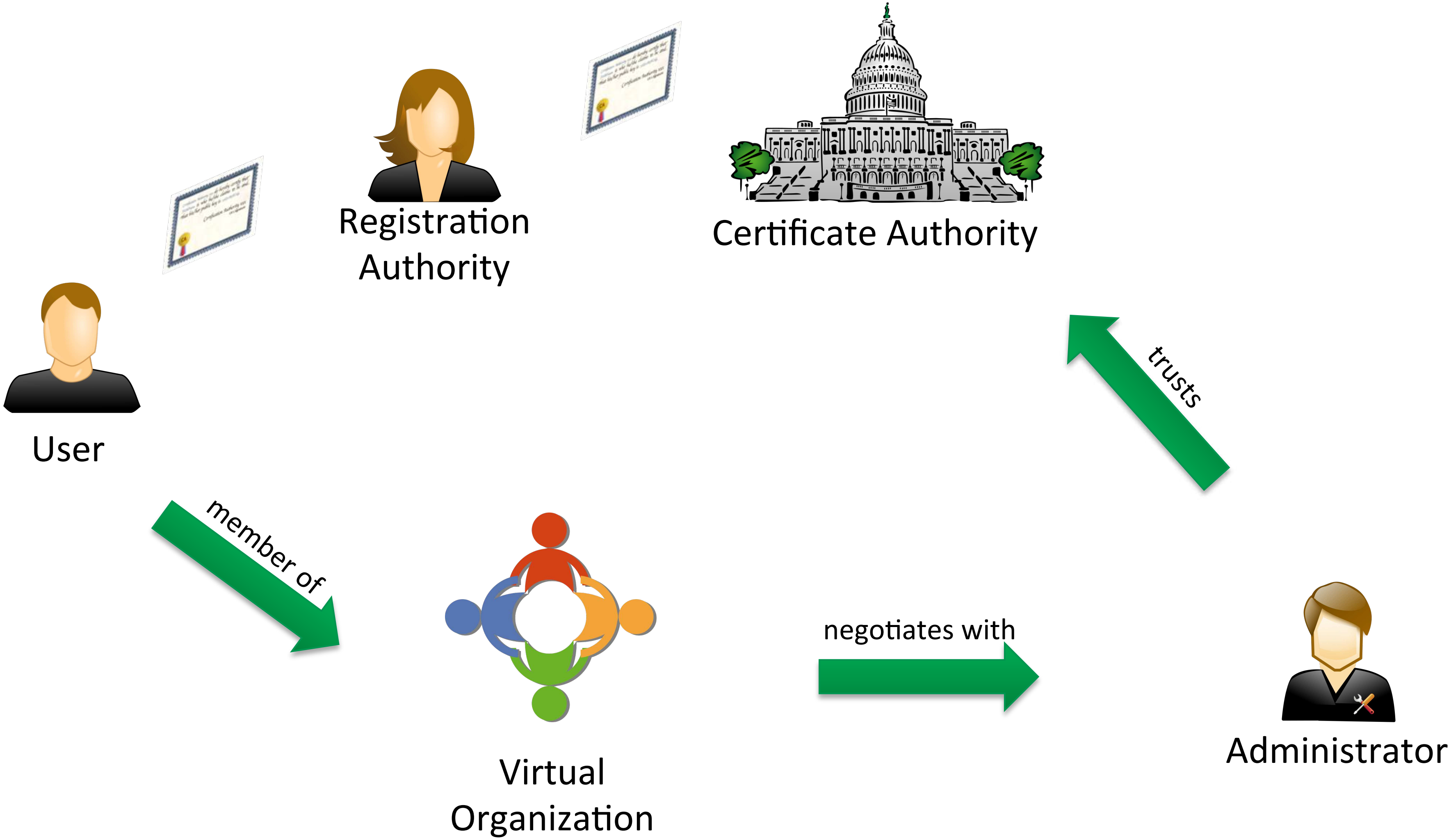
Outline

- ❑ Authentication vs. Authorization
- ❑ Grid Security Infrastructure (GSI)
- ❑ Certificates
  - Personal X509 certificates
  - CA certificates
- ❑ Delegation
  - Proxy generation
  - VOMS extension – LCMAPS
  - Myproxy renewal



Authentication vs. Authorization

The grid security trust chain



Registration Authority

Certificate Authority

User

trusts

member of

negotiates with

Virtual Organization

Administrator

Grid Security Infrastructure I

- **Grid security is hard**
  - Authentication & Service-to-service interactions
  - Authorization & VO policies
  - Transparency & Standardization of interfaces
  - Organizational Trust

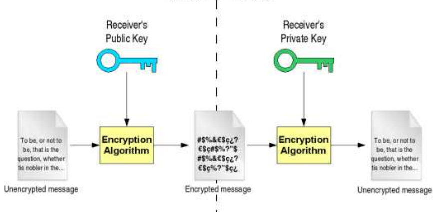
- **Key requirements for GSI**
  - Data confidentiality
  - Data Integrity
  - Delegation & Single-Sign-On

Grid Security Infrastructure II

- GSI core module is

Asymmetric Key Cryptography

- X509 certificate
- CA certificate
- Secure Sockets Layer (SSL)
- VOMS privileges
- Proxy delegation


Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the...
Encryption Algorithm
#$%&€$ç¿? €$ç#$%?"$ #$%&€$ç¿? €$ç%?"$ç¿
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the...
Unencrypted message
Encrypted message
Unencrypted message

X.509 anatomy

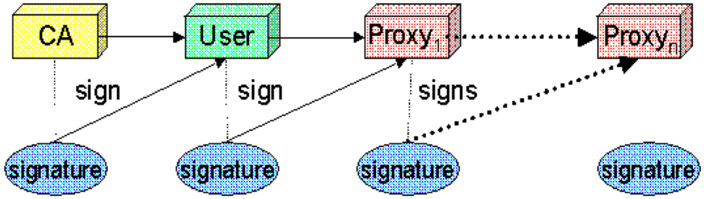
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 433 (0x1b1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=org, DC=egee-ne, OU=Training Services, CN=Worthless EGEE Northern and Benelux Tutorial CA 1
        Validity
            Not Before: Oct  6 07:03:58 2013 GMT
            Not After : Dec  6 07:03:58 2013 GMT
        Subject: DC=org, DC=egee-ne, O=Training Services, OU=users, CN=MOOC
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ca:6d:7f:bc:4b:fb:c4:a4:db:7c:bc:c7:a5:a1:
                    e0:4d:77:83:da:dc:c4:17:28:5e:cb:ba:83:35:fa:
                    47:5f:04:06:f0:2b:dd:c0:26:af:24:5c:58:9f:08:
                    bb:47:54:55:8f:65:03:aa:60:c5:63:f1:3c:f9:dc:
                    64:8a:ac:b2:6e:42:4d:43:20:87:93:9e:4c:2d:3e:
                    2b:79:b8:a4:4d:72:2a:6e:67:43:9e:8e:d2:ee:f5:
                    4d:03:e1:92:8b:d1:2d:33:ca:56:b4:56:d3:31:9d:
                    ba:57:38:75:77:a9:62:22:cd:c1:e0:55:9d:9d:02:
                    f8:e0:90:62:f3:22:3f:bb:07
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ca.dutchgrid.nl/egee-ne/cacrl.der
```

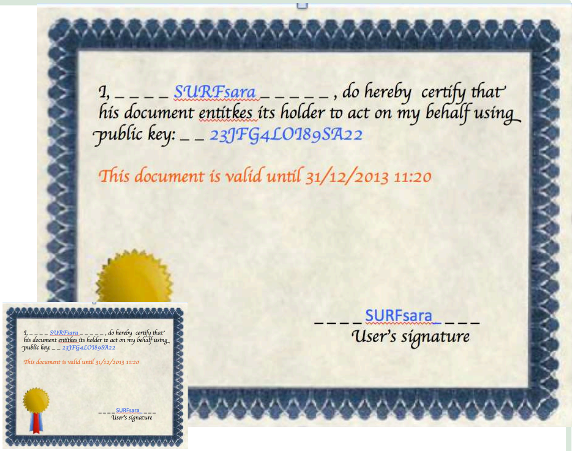
```
    Signature Algorithm: sha1WithRSAEncryption
        41:d7:5a:ca:28:bc:84:f7:7c:ba:bb:01:f8:7d:50:a0:c1:7e:
        4d:f4:b7:b3:8e:d6:20:78:0b:67:5a:b2:b5:ed:76:eb:fa:88:
        d1:9b:59:3c:68:7c:4a:7c:8e:12:17:9f:b8:54:85:f5:5d:b3:
        2b:d1:94:b7:d9:3e:06:61:a1:f1:03:72:b3:09:98:c1:4e:d8:
        e7:2f:0d:0f:03:72:f0:20:0d:26:67:4d:f1:66:f2:8a:55:bd:
        9a:3e:a9:50:19:f1:f7:f0:1e:5e:a4:0e:92:1b:0c:e8:e1:a3:
        ae:42:9e:a1:72:00:9a:3b:5f:99:1a:5a:a6:cd:53:25:ab:6d:
        2a:e5
```

```
-----BEGIN CERTIFICATE-----
MIIDRDCCAq2gAwIBAgICAbEwDQYJKoZIhvcNAQEFBQAwgYYxEzARBgoJkiaJk/Is
ZAEZEwNvcmcxFzAVBgoJkiaJk/IsZAEZEwdlZ2VlLW5lMRowGAYDVQQLExFUcmFp
bmluZyBTZXJ2aWNlczE6MDgGA1UEAxMxV29ydGhsZXNzIEVHRUUgTm9ydGhlcm4g
YW5kIEJlbmVsdXggVHV0b3JpYWwgQ0EgMTAeFw0xMzEwMDYwNzAzNThaFw0xMzEy
MDYwNzAzNThaMGkxEzARBgoJkiaJk/IsZAEZFgNvcmcxFzAVBgoJkiaJk/IsZAEZ
FgdlZ2VlLW5lMRowGAYDVQQKExFUcmFpbmluZyBTZXJ2aWNlczEOMAwGA1UECxMF
dXNlcnMxDTALBgNVBAMTBE1PT0MwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AMptf7xL+8Sk23y8x6Wh4E13g9rcxBcoXsu6gzX6R18EBvAr3cAmryRcWJ8Iu0dU
VY9lA6pgxWPxPPncZIqssm5CTUMgh5OeTC0+K3m4pE1yKm5nQ56O0u71TQPhkovR
LTPKVrRW0zGdulc4dXepYiLNweBVnZ0C+OCQYvMiP7sHAgMBAAGjgdwwgdkwDAYD
VR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBLAwEwYDVR0lBAwwCgYIKwYBBQUHAwIw
OQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2NhLmR1dGNoZ3JpZC5ubC9lZ2VlLW5l
L2NhY3JsLmRlcjBpBglghkgBhvhCAQ0EXBZaVGhpcyBpcyBhIFdvcnRobGVzcyBU
dXRvcmlhbCBDZXJ0aWZpY2F0ZTogdGhlIG93bmVyIGhhcyBub3QgYmVlbiBhdXRo
ZW50aWNhdGVkIGluIGFueSB3YXkuMA0GCSqGSIb3DQEBBQUAA4GBAEHXWsoovIT3
fLq7Afh9UKDBfk30t7OO1iB4C2dasrXtduv6iNGbWTxofEp8jhIXn7hUhfVdsyvR
lLfZPgZhofEDcrMJmMFO2OcvDQ8DcvAgDSZnTfFm8opVvZo+qVAZ8ffwHl6kDpIb
DOjho65CnqFyAJo7X5kaWqbNUyWrbSrl
-----END CERTIFICATE-----
```

Delegation



- ❑ **Delegation**
  - Create proxy
    - ✓ New key pair
    - ✓ Limited lifetime
  - A generates a proxy with a mutually agreed key pair with B. Then B acts on behalf of A and C who trusts A, trusts also B.

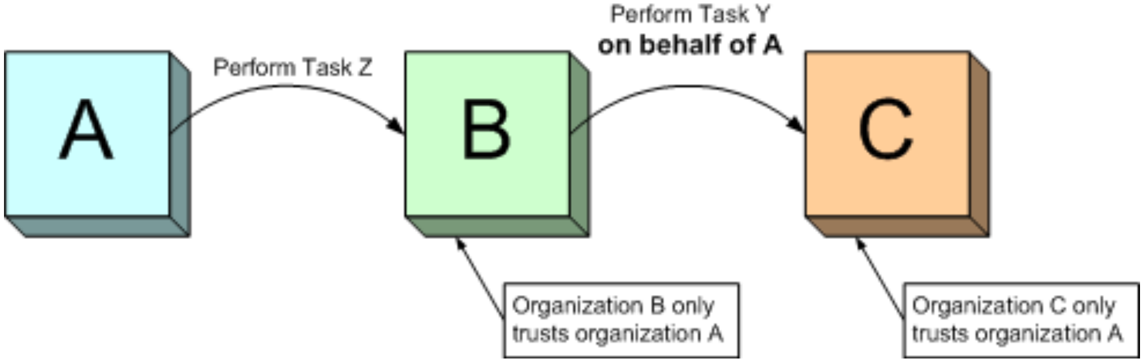


I, ____ SURFsara ______, do hereby certify that his document entitkes its holder to act on my behalf using public key: __ 23JFG4LO189SA22

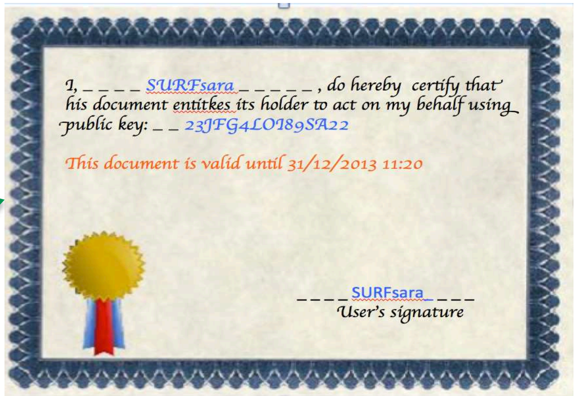
This document is valid until 31/12/2013 11:20

____SURFsara___
User's signature

- ❑ **Single Sign On**
  - Less pass-phrases


A
B
C
Perform Task Z
Perform Task Y
on behalf of A
Organization B only trusts organization A
Organization C only trusts organization A

Proxy generation

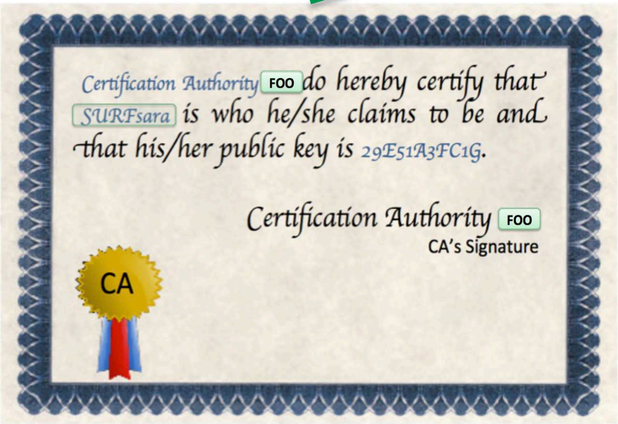


I, _ _ _ _ SURFsara _ _ _ _ _ _ , do hereby certify that his document entitkes its holder to act on my behalf using public key: _ _ 23JFG4LO189SA22

This document is valid until 31/12/2013 11:20

_ _ _ _ SURFsara_ _ _ _
User's signature

SURFsara signs the proxy

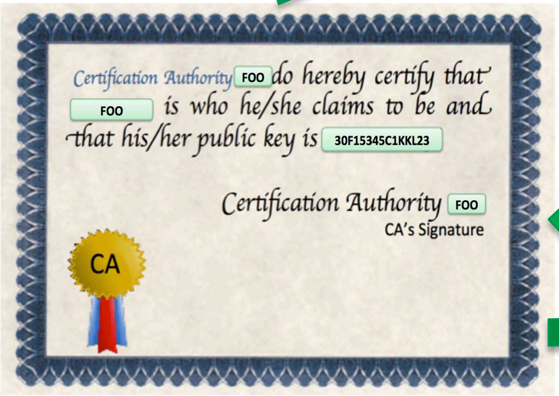


Certification Authority FOO do hereby certify that SURFsara is who he/she claims to be and that his/her public key is 29E51A3FC1G.

Certification Authority FOO
CA's Signature

CA

CA ***FOO*** signs SURFsara's certificate



Certification Authority FOO do hereby certify that FOO is who he/she claims to be and that his/her public key is 30F15345C1KKL23

Certification Authority FOO
CA's Signature

CA

CA ***FOO*** signs its own certificate

VOMS extension

- VO-extensions – *authorization*

- VOMS (VO Management Service):
  - User roles and privileges in a VO
  - Certificate extension
  - VOMS server returns attributes
    - ✓ VO membership
    - ✓ Associated roles

MyProxy

- ❑ **Problem: jobs > 12h fail**

- ❑ **Solution: Myproxy certificate**
  - Creates proxy for 1 week
  - Stores the proxy to a server called Myproxy
  - WMS contacts Myproxy for renewal every 12 h
  - Renewal achieved without a passphrase

Summary

- Certificates enable authentication
- VOMS extensions enable authorization
- Proxy certificates are used to shield your real certificate
- The MyProxy service enables longer life time jobs