Grid certificates for users in Switzerland

Accrediting QuoVadis with EuGridPMA and IGTF

SWITCH

Serving Swiss Universities

Alessandro Usai
alessandro.usai@switch.ch

Why do we need it?

Switzerland is currently involved in many grid projects e.g. EGEE, Swing and as such it is important to be recognized as a CA by EuGridPMA (European Policy Management Authority for Grid Authentication) so as to have access to the distributed grid resources.

We have three kind of certificates:

- 1 year User Certificates
- 1 year Host Certificates
- Short Lived Credential Certificates (SLCS)

IGTF/EUGridPMA bundle

- A tar file/rpm with the trusted CA: the bundle contains the CA root certificates, CRL information as well as policies files.
- The bundle is typically installed by all the Grid relying parties on all their grid nodes e.g. EGEE, and this is also currently true for Swing/SMSCG.

How do we get accredited?

- Request through EuGridPMA, which is a “club” of CAs who agree on members/policies/procedures.
- QuoVadis will be officially presented to them at the next meeting (one every 3 months) in Lisbon (6–8 October): the aim is to have the accreditation finalized in the EuGidPMA bundle by May 2009 the latest.

- The application (CP/CPS) is checked iteratively by the relying parties and eventually accepted, after all the requested amendments are applied. The iteration can last few months.
- Final acceptance always finalized at a EuGridPMA meeting (hopefully either Cyprus in January 2009 or Zurich in May 2009)

What do the grid certificates look like?

- User Certificate example
- Host certificate example
- Issuing CA Certificate example

- Notice In particular that:
  - common prefix for all Grid certs:
  - DC=com, DC=quovadisglobal, DC=grid

  - prefix for SWITCH user certs:
  - DC=com, DC=quovadisglobal, DC=grid, DC=switch, DC=users

  - prefix for SWITCH server certs:
  - DC=com, DC=quovadisglobal, DC=grid, DC=switch, DC=hosts

End-entity Certificate (1/2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 31 (0x1f)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BM, O=QuoVadis Limited, CN=QuoVadis Grid ICA
        Validity
            Not Before: Aug 26 08:41:25 2008 GMT
            Not After : Aug 26 08:41:25 2009 GMT
        Subject: DC=com, DC=quovadisglobal, DC=grid, DC=switch, DC=users,
                 O=SWITCH, CN=Alessandro Usai
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    …
```

End-entity Certificate (1/2)

```
X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.8024.0.1
                Policy: 1.2.840.113612.5.2.2.1.4
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                email:alessandro.usai@switch.ch
            X509v3 Subject Key Identifier:
                …
            X509v3 Authority Key Identifier:
                keyid:…
            X509v3 CRL Distribution Points:
                URI:http://crl.quovadisglobal.com/qvgica.crl
            Authority Information Access:
                CA Issuers - URI:http://trust.quovadisglobal.com/qvgica.crt
```

Host Certificate (1/2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 33 (0x21)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BM, O=QuoVadis Limited, CN=QuoVadis Grid ICA
        Validity
            Not Before: Aug 27 08:33:18 2008 GMT
            Not After : Aug 27 08:33:18 2009 GMT
        Subject: DC=com, DC=quovadisglobal, DC=grid, DC=switch, DC=hosts,
                 O=SWITCH, CN=server.switch.ch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                …
```

Host Certificate (2/2)

```
X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.8024.0.1
                Policy: 1.2.840.113612.5.2.2.1.4
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Authority Key Identifier:
                keyid:…
            X509v3 Subject Key Identifier:
                …
            X509v3 CRL Distribution Points:
                URI:http://crl.quovadisglobal.com/qvgica.crl
            Authority Information Access:
                CA Issuers - URI:http://trust.quovadisglobal.com/qvgica.crt
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:server.switch.ch
```

Issuing CA Certificate (1/2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 13 (0xd)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BM, O=QuoVadis Limited, CN=QuoVadis Root Certification
                Authority
        Validity
            Not Before: Aug 26 17:01:51 2008 GMT
            Not After : Aug 24 17:01:51 2018 GMT
        Subject: C=BM, O=QuoVadis Limited, CN=QuoVadis Grid ICA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                …
```

Issuing CA Certificate (2/2)

```
X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:…
            X509v3 Subject Key Identifier:
                …
            X509v3 CRL Distribution Points:
                URI:http://crl.quovadisglobal.com/qvrca.crl
            Authority Information Access:
                CA Issuers - URI:http://trust.quovadisglobal.com/qvrca.crt
```

Switch Requirements (1/2)

- Certificate lifetime of at least ten years for the Issuing CA
- End Entities and Server certificates lifetime of no more than 13 months.
- Any further certificate policies extension for the Issuing CA certificate must not include a URI.
- No intermediate certificate with a key longer than 2048 bits (QuoVadis Root CA 1).
- The issuing CA CRL lifetime will be of at least 7 days.
- No OCSP (Online Certificate Status Protocol) responder URI in the Grid certificates, at least initially.

Switch Requirements (2/2)

Identity vetting requirements:

- It should be enough to rely on copies of identity documents sent by either fax or email for identity vetting, whenever the requests are from trustworthy partners institutions.
- We would like to have procedures which require as little paper handling as possible e.g. digitally signed e-mail from a proxy of the organization.

What will change?

- SwissSign hierarchy cumbersome e.g. we will not need a safe in a bank anymore:)
- Less hassle as we will NOT have the email field in the certificates.
- Easier to manage the portal and to nominate RAs.
- Less paper work to handle

What will not change?

- SLCS is not affected by the transition as the root CA is hosted/managed by SWITCH!

RA procedures: we need your feedback :)

- What do you envisage? What should be definitely provided and which is currently not?
- What did you not like so far?

SLCS ACL: HOW TO

For an exhaustive tutorial have a look at

http://www.switch.ch/grid/slcs/documents/webadmin/index.html

In particular, the access point for the production SLCS ACL is

https://slcs.switch.ch/SLCS/admin/

In case of any problems, the first question/action always is: What are your attribute values?

To find out go to https://aai-viewer.switch.ch/

SLCS Identity vetting requirements (1/2)

Look at the CP/CPS document:

http://www.switch.ch/grid/slcs/documents/

from which:

3.2 Initial identity validation The initial identity validation consists of the following steps:

- the requester contacts the RA of his Identity Provider in order to obtain permission to access the SWITCHslcs service
- the RA enables access to the SWITCHslcs service for the requester upon confirmation that the following two requirements are fulfilled:
  a) the individual has a valid SWITCHaai account

SLCS Identity vetting requirements (2/2)

b) the account creation was dependent on a process which had one of the following properties:

1) Issuance of an identity card, which gives its holder monetary benefits
2) the account has a direct relation to human resources data, which is used for salary payments
3) a registration process with the RA, which included submission of a copy of a passport or other official identity card.

– The requester can access the SWITCHslcs website and obtain his/her short-lived certificate upon successful authentication at his/her Identity Provider.

The RAs devise their own registration process in order to ensure the two requirements a) and b) as stated above are fulfilled.

The SWITCHslcs service allows the RA to allow as well as prohibit access to the SWITCHslcs service for its users.

SLCS ACL Demo

Test Environment

https://hestia.switch.ch/SLCS/admin

Notice the path /admin (≠/login) with which you login as admin (after which you see by default the groups you can manage)

Notice also that:

- you cannot add a group
- you cannot add another administrator
- These two actions require editing an xml file on the server