SWITCH

The Swiss Education & Research Network

Being/becoming a SWITCHpki RA operator: expectations, obligations and privileges

Kaspar Brand
SWITCH

A SWITCHpki RA operator…

SWITCH
The Swiss Education & Research Network

… is the central point of contact at an organization for PKI related inquiries (for employees/students of this organization as well as for SWITCH)

… is expected to be familiar with PKI basics (confidentiality, authentication, integrity, non-repudiation), SSL/TLS certificates and the SWITCH CP/CPS

… should have at least one substitute at his organization

… is typically a member of the IT department staff

… has the authority to approve or reject a request for a certificate which includes the name of his organization in the subject (O=…)

… will be blamed (and his organization held liable) if he has approved a fraudulent request

… is a cornerstone for assuring the quality of SWITCHpki certificates

What is put into a certificate?

SWITCH
The Swiss Education & Research Network

In ASN.1 lingo, a certificate looks like this (excerpt from RFC 3280):

```
Certificate  ::=  SEQUENCE  {
   tbsCertificate       TBSCertificate,
   signatureAlgorithm   AlgorithmIdentifier,
   signature            BIT STRING  }
TBSCertificate  ::=  SEQUENCE  {
   version         [0]  Version DEFAULT v1,
   serialNumber         CertificateSerialNumber,
   signature            AlgorithmIdentifier,
   issuer               Name,
   validity             Validity,
   subject              Name,
   subjectPublicKeyInfo SubjectPublicKeyInfo }
```

➔ As an RAO, you primarily care about the requested **subject name**

How does a certificate subject look like?

SWITCH
The Swiss Education & Research Network

The certificate subject is a sequence of attributetype-value pairs called **Relative Distinguished Names (RDN)** which together form a **Distinguished Name (DN):**

C=CH, O=Switch - Teleinformatikdienste fuer Lehre und Forschung, CN=www.switch.ch
(sometimes also written as
/C=CH/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=scs.switch.ch)

DNs have their origins in the X.500 standards family, common RDNs are *countryName, stateOrProvinceName, localityName, organizationName, organizationalUnitName, commonName*

For servers, the **commonName (CN)** and **organizationName (O)** are the most important RDNs. The CN attribute must contain a fully qualified domain name (FQDN), and its domain must be associated with the organization specified by the O attribute.

Subject alternative names

SWITCH
The Swiss Education & Research Network

Introduced by RFC 2459 (1999, now obsoleted by RFC 3280) as an X.509v3 extension:

```
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER}
```

Most relevant for server certificates: dNSName (possibly iPAddress), for personal certificates: rfc822Name (= e-mail address)

dNSNames currently supported with SwissSign certificates, expected to become available with SCS certificates by mid-year

How does a request look like?

SWITCH
The Swiss Education & Research Network

… on the SwissSign registration form:

2 Certificate Request

The customer submits a certificate request with the following information:

Purpose: Server Identity Certificate
Content: Real Information
Profile:
Req. ID: C4B76FBF6677898C
Key ID: AB78C0CD2A6E06218251885FC3BB2C2F96D397D7

3 Individual Information

The customer requires the following identifying information to be added to the certificate:

/CN= www.olat.org
/Email= id_olat@id.unizh.ch

As proof of the individual information, the customer will submit the following documentation

- Photo Identity (passport, driver… identity card) of the individual signing in
- WHOIS Record for server certificates and photo identity of the individual signing in 6.b)

4 Organizational Information

The customer requires the information in the certificate to

/O = Universitaet Zuerich
/C = CH

As proof of the organizati… customer will submit th… documentation

- Excerpt from the commercial re… photo identity of the individual …

5 Optional Information

These optional fields will be added a…

DNS:www.olat.org,DNS:olat.org

/OU= will only be added if organizational …formation has been included.

6 Customer Authorization

a) To authorize the use of the identity information and to confirm the correctness of the information, please sign here:	Location: Signature:
b) To authorize the use of the WHOIS information and to confirm the correctness of the information, please sign here:	Location: Signature:
c) To authorize the use of the organizational information and to confirm the correctness of the information, please sign here:	Location: Signature:

4 Organizational Information

The customer requires the organizational information in the certificate to be as follows:

/O = Universitaet Zuerich
/C = CH

As proof of the organizational information, the customer will submit the following documentation

- Excerpt from the commercial register and photo identity of the individual signing in 6.c)

5 Optional Information

These optional fields will be added as well:

DNS:www.olat.org,DNS:olat.org

3 Individual Information

The customer requires the following identifying information to be added to the certificate:

/CN= www.olat.org
/Email= id_olat@id.unizh.ch

As proof of the individual information, the customer will submit the following

Obligations as RAO at your organization

SWITCH
The Swiss Education & Research Network

Determine if the applicant is entitled to request a certificate

Check that the subject is correct (DNS domain in common Name, and subjectAltName[s], name of organization)

Request a copy of an official photo identity document (passport, ID card, driver's license, student ID – upon first-time registration only, or when the archived copy has expired)

Keep an archive of the documents related to the certificate request (registration form, copies of photo identity documents)

If RAO with access to CA Web frontend: properly secure access to your RAO certificate (private key on HW or soft token)

How does a request look like? (cont.)

SWITCH
The Swiss Education & Research Network

… on the GlobalSign WebConnect RA interface:

SureServerEDU_TLS_3year - GlobalSign SWITCH - Edit Pending Certificate Order

Issue certificate order | Defer certificate order | Deny certificate order

Cert Order details

ID : 824588429
Status : Not verified
Ordered on : Mon, March 20 2006, 09:29 GMT Details
Public certificate : Yes

Request details

Status : No matching certificates yet
Received on : Mon, March 20 2006, 09:29 GMT Details
Type : Standard PKCS10
Key size : 2048 bits
Request : MIICrDCCAZQCAQAwZzELMAkGA1UEBhMCQ0gxQDA+BgNVBAoTN1N3aXRjaCAtIFRl
bGVpbmZvcm1hdGlrZGllbnN0ZSBmdWVyIExlaHJlIHVuZCBGb3JzY2h1bmcxFjAU
BgNVBAMTDXd3dy5zd2l0Y2guY2gwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDtFiVM0nbSxqeFPevZt8JEtu0wfjdtyFkEu4josUuWU8bRi7xmroCVNZTh
s/Cq6Y6/Zo+vYVlXfALl4UpeJQf3pL/8+5/8OqDIuMEjAconCj2VXpZvoY8xOfy0
5NxCl4hj2NqUiHYv5tVZV7zupZx8Adqs63V+e1f0shN4nSK3rEfFhMrn64lL47G/
BdESOh9uS/EmE1MOWv/oVxUiHxnTOlh5FEAmP1JANEu+rOcLnem18TqUPiruUPBs
upDwu8R1gF9L ap8Fy0fDoRu7kW/fRl9L6SYnx0cJ8g
sY9sG1x0yZKjI EBkGebI2QXp3VzKDFDy0nMo4Q6BrOKj
G9Xx5ehPZuoP zcsSbDtRH4n5T+BuvwbUkapgTIvSG1pztJJ3P+3Is
rFD3Kha55iMqG kRA==

Subject : countryName=CH, organizationName=Switch - Teleinformatikdienste fuer Lehre und Forschung,
commonName=www.switch.ch

Subject : countryName=CH, organizationName=Switch - Teleinformatikdienste fuer Lehre und Forschung,
commonName=www.switch.ch

RA operator privileges

SWITCH
The Swiss Education & Research Network

At organizations operating their own registration authority, the RA operator has full control over the certificate life-cycle:

- direct access to the Web frontend of the CA (SwissSign/GlobalSign)
- approve certificate requests (with immediate effect)
- revoke certificates
- search for certificates
- download reports of certificates issued to own organization

Being a recognized contributor to the success of SWITCHpki…

… and getting invited to exclusive SWITCHpki RAO meetings ☺

The Swiss Education & Research Network