The SWITCHpki RA Operator

Role and responsibilities

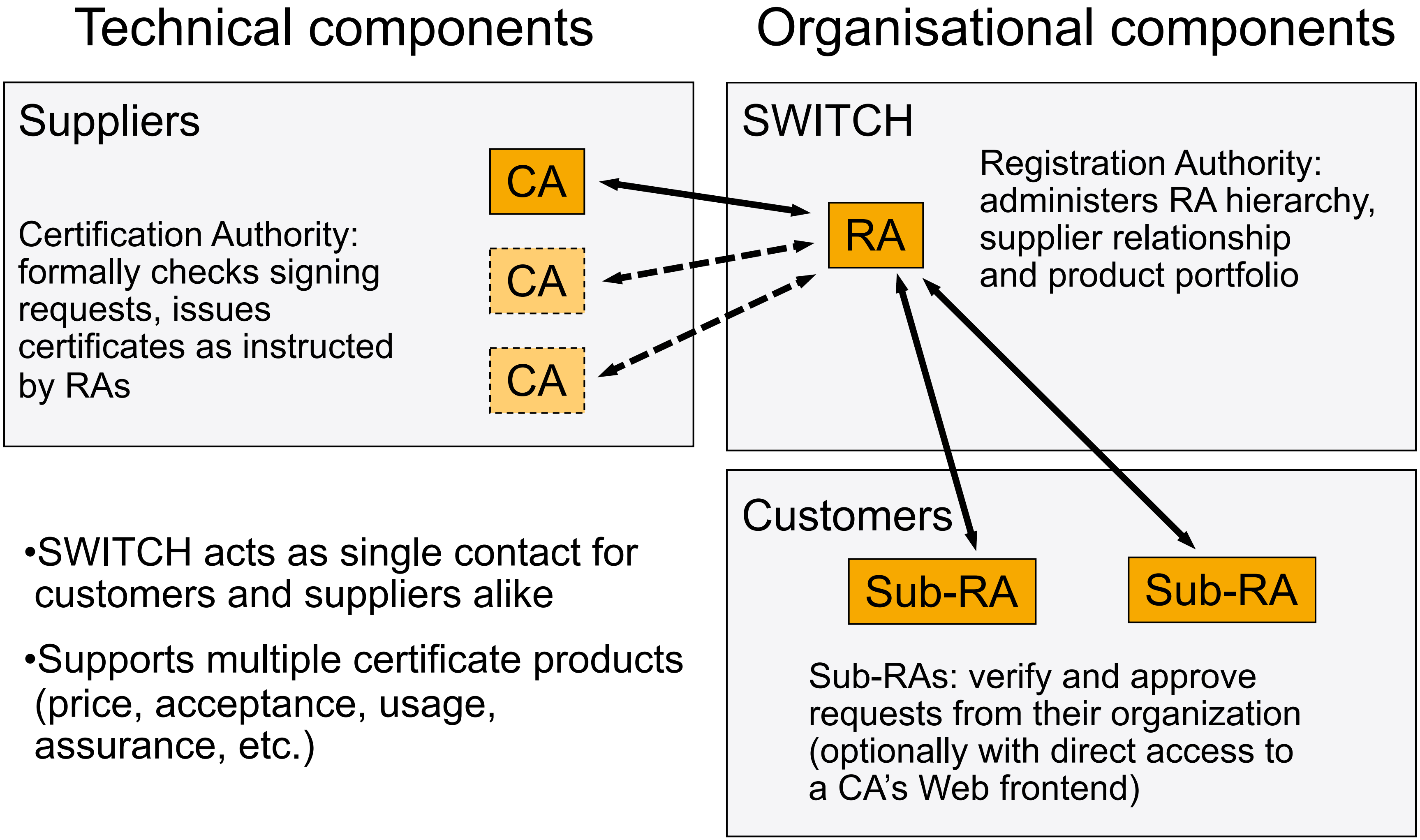
SWITCHpki Team
pki@switch.ch

November, 2016

Structure of SWITCHpki

- A **P**ublic **K**ey **I**nfrastructure for the Swiss higher education system (universities, federal institutes of technology, universities of applied sciences)
- Based on two main components:
  - The **Certification Authority (CA),** which encompasses the technical infrastructure for issuing certificates
  - The **Registration Authority (RA),** which is responsible for checking and confirming the correctness of certificate requests
- CA operations is outsourced to commercial suppliers (*QuoVadis*)
- RA is run by SWITCH *and* the participating organizations (by signing the agreement, the organizations become [Sub-]RAs)

SWITCHpki service concept



Technical components

Organisational components

Suppliers

Certification Authority: formally checks signing requests, issues certificates as instructed by RAs

SWITCH

Registration Authority: administers RA hierarchy, supplier relationship and product portfolio

Customers

Sub-RAs: verify and approve requests from their organization (optionally with direct access to a CA’s Web frontend)

- SWITCH acts as single contact for customers and suppliers alike
- Supports multiple certificate products (price, acceptance, usage, assurance, etc.)

Available types of certificates (1)

Server Certificates

- Business SSL
  - For generic SSL/TLS enabled applications: Web servers (HTTP), directory servers (LDAP), Mail servers (IMAP, POP, SMTP), AAI (Shibboleth), RADIUS servers, …
  - Available with 1-, 2- or 3-year validity
  - Up to 50 DNS names allowed
- Extended Validation (EV) SSL
  - Recommended in particular for Web sites for “human” visitors, and where sensitive data is transmitted (e.g. IdP login page, HR admin database or similar)
  - Available with 1- or 2-year validity
  - Up to 20 DNS names allowed

Available types of certificates (2)

User Certificates

- Advanced Personal Certificates
  - For e-mail signing/encryption and web client authentication
  - Available to persons (if offered by your organisation at all)
  - Provided as soft-token certificate (installed on client)
  - Not suitable for signing PDF documents (requires hard-token certificate)
  - Validity up to 3 years

Server Certificates: Validation Types

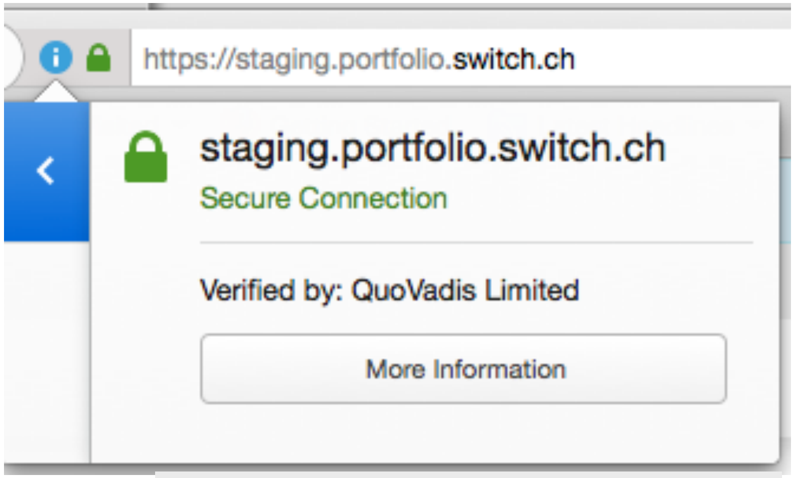
- **DV: Domain validated** *(not available in SWITCHpki)*
  - Validation via e-mail exchange with contact listed in Whois record, or validation via evidence on website or in DNS records of domain
  - Weak validation

- **OV: Organization validated** (*Business SSL* certificate)
  - Validation of existence of organization (via Commercial Registry, law, contract, etc.)
  - Strong validation (repeated every 3 years)

- **EV: Extended validation** *(Extended Validation (EV) SSL certificate)*
  - Extended validation of existence of organization (via Commercial Registry, law, contract, etc.), including validation of Person's roles, phone numbers, etc.
  - Extra strong validation (repeated every year)

"Standard" (OV) SSL vs. EV SSL

Firefox



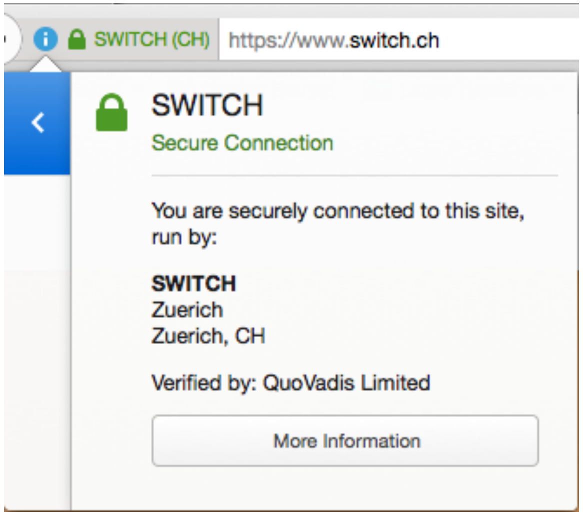
https://staging.portfolio.switch.ch

staging.portfolio.switch.ch

Secure Connection

Verified by: QuoVadis Limited

More Information



SWITCH (CH) https://www.switch.ch

SWITCH

Secure Connection

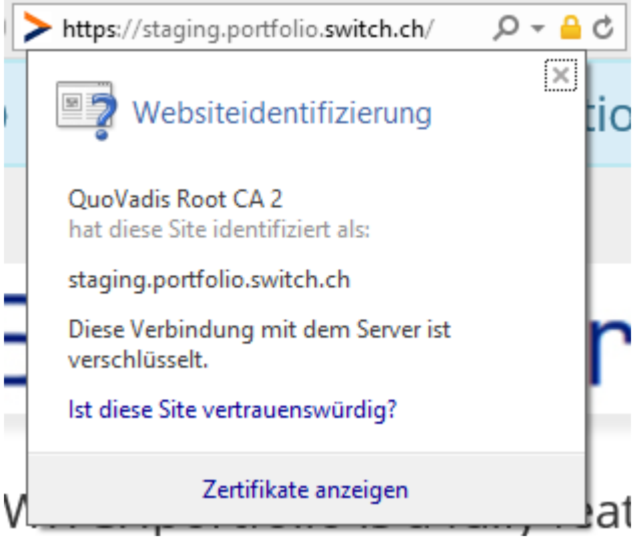
You are securely connected to this site, run by:

SWITCH
Zuerich
Zuerich, CH

Verified by: QuoVadis Limited

More Information

Internet Explorer



https://staging.portfolio.switch.ch/

Websiteidentifizierung

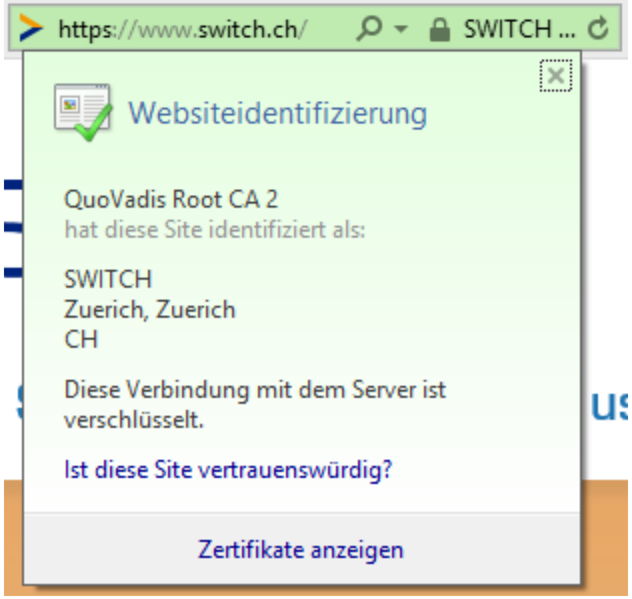
QuoVadis Root CA 2
hat diese Site identifiziert als:

staging.portfolio.switch.ch

Diese Verbindung mit dem Server ist verschlüsselt.

Ist diese Site vertrauenswürdig?

Zertifikate anzeigen



https://www.switch.ch/ SWITCH ...

Websiteidentifizierung

QuoVadis Root CA 2
hat diese Site identifiziert als:

SWITCH
Zuerich, Zuerich
CH

Diese Verbindung mit dem Server ist verschlüsselt.

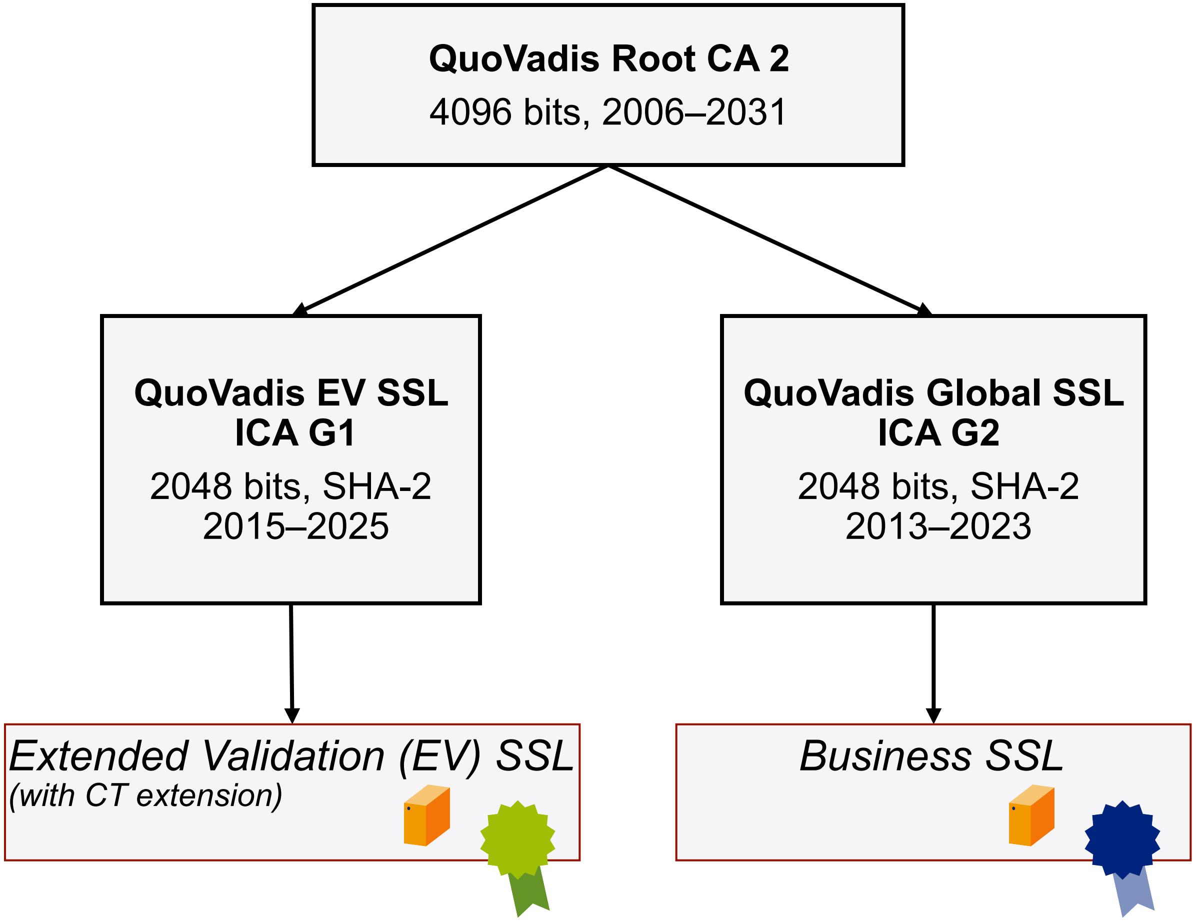
Ist diese Site vertrauenswürdig?

Zertifikate anzeigen

https://evct.ssl.switch.ch/

The QuoVadis CA certificate hierarchy (1)

Server Certificates



QuoVadis Root CA 2
4096 bits, 2006–2031

QuoVadis EV SSL ICA G1
2048 bits, SHA-2
2015–2025

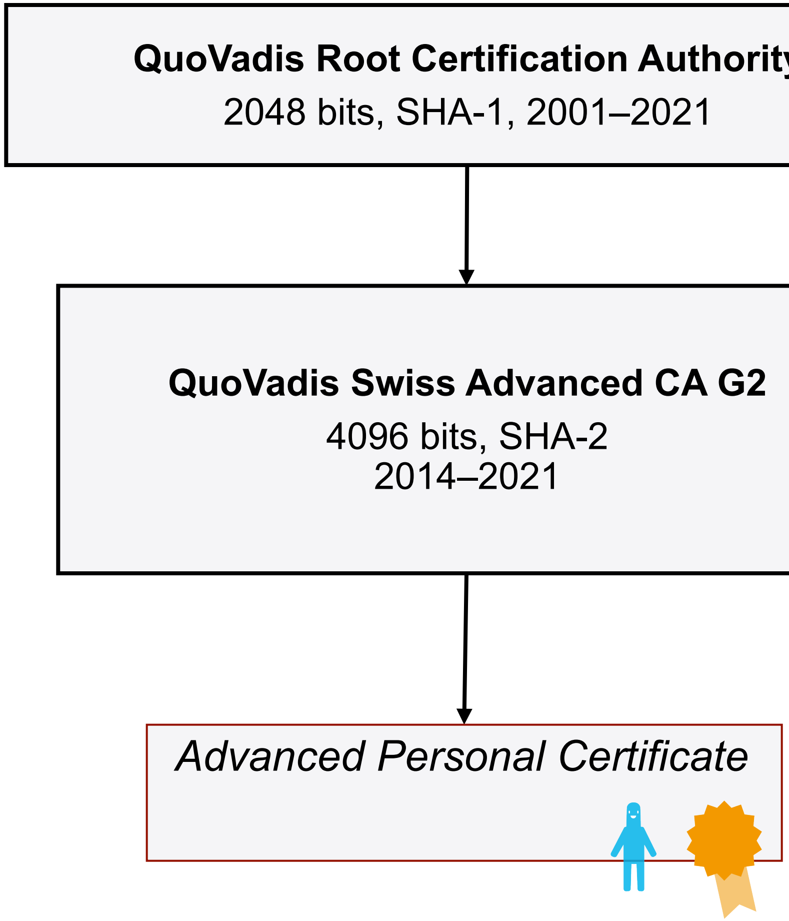
QuoVadis Global SSL ICA G2
2048 bits, SHA-2
2013–2023

Extended Validation (EV) SSL
(with CT extension)

Business SSL

The QuoVadis CA certificate hierarchy (2)

User Certificates



QuoVadis Root Certification Authority
2048 bits, SHA-1, 2001–2021

QuoVadis Swiss Advanced CA G2
4096 bits, SHA-2
2014–2021

Advanced Personal Certificate

QuoVadis root certificate preinstallation

- Operating systems
  - Microsoft Windows (XP and later)
  - Apple OS/X (10.2/Jaguar and later)
  - All major Linux distributions
  - iPhone OS (2.0 and later)
  - Android (1.6 and later)
  - Windows Phone 7
- Applications/Toolkits
  - Microsoft Internet Explorer (5.0 and later), Microsoft Outlook
  - Firefox (1.0.2 and later), Thunderbird (1.0.2 and later), ...
  - Google Chrome
  - Apple Safari (1.0 and later)
  - Opera (9.26 and later)
  - Sun JDK/JRE (1.4.2_22/1.5.0_20/1.6.0_15 and later)
  - Adobe Acrobat (versions 9.x and later)

Well supported

The SWITCHpki RA operator…

- 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 typically a member of the IT department staff, should have at least one substitute
- Is expected to be familiar with PKI basics, SSL/TLS and X.509 certificates
- Is aware of the CP/CPS and related documents
- Has the authority to approve or reject a request for a certificate for his own organization (subject with O=…)
- Will be blamed (and his organization held liable) if he has approved a fraudulent request

RA operator duties

- Determine if the applicant is entitled to request a certificate (employee/student of the organization?)
- Check that the submitted request is legitimate/genuine
- For user certificates: make sure that a valid copy of an official photo identity document (passport, ID card) is submitted together with the request
- Keep an archive of those documents which are not forwarded to SWITCH (e.g. copies of internal e-mail correspondence, for Sub-RAs under the RA Bulk model also copies of photo ID documents etc.)
- For RA operators with admin certificates: properly secure the access to the private key (protect with passphrase)

The subject of a certificate request

- The subject is the most important part of a certificate signing request (CSR), together with the requested entries for the subjectAltName extension
- The subject DN (Distinguished Name) is composed of multiple attributetype-value pairs called RDNs (Relative Distinguished Names:

```
C=CH, O=Universite de Geneve, CN=idp.unige.ch
C=CH, O=Haute Ecole Specialisee de Suisse occidentale (HES-SO), CN=pwlan.hefr.ch
C=CH, O=Universita della Svizzera Italiana, CN=login.unisi.ch
```

- Common RDNs include *countryName (C), stateOrProvinceName (ST), localityName (L), organizationName (O), organizationalUnitName (OU), commonName (CN)*
- Subject and subjectAltName entries **must be carefully checked** by the RA operator before any approval

Checking a request

- Many checks are already applied when a CSR is submitted through the form on www.switch.ch
  - Parameters of the key (only RSA keys are accepted)
    - ❑ Key size (either 2048 or 4096 bits)
    - ❑ Exponent > 65536
    - ❑ No known weak keys (CVE 2008-0116 aka Debian OpenSSL)
  - Subject DN: at least a CN attribute with a “proper” FQDN
  - Domains of requested FQDNs and e-mail address syntax
  - Correct ASN.1 encodings (causes warnings only)
  - EV SSL eligibility (per organization and domain)
  - Supported vs. unsupported RDNs (e.g. *description*, *unstructuredName*)
- The ***organizationalUnitName*** **(OU=) attribute** can’t be checked in an automated way (against a list of known acceptable values), so it **needs manual verification by the RA operator**

In short

- For request confirmation, SWITCHpki depends on RA operators at each participating organization
- Careful verification of the requested subject DN and subjectAltName entries is a crucial step before approving any SWITCHpki certificate request
- It’s the responsibility of each participating organization to make sure that no bogus requests are approved by its RA operators (can be held liable otherwise)
- RA operators are the cornerstone for assuring the quality of SWITCHpki certificates