Obtaining QuoVadis certificates from SWITCH

Products and Procedures

Serving Swiss Universities

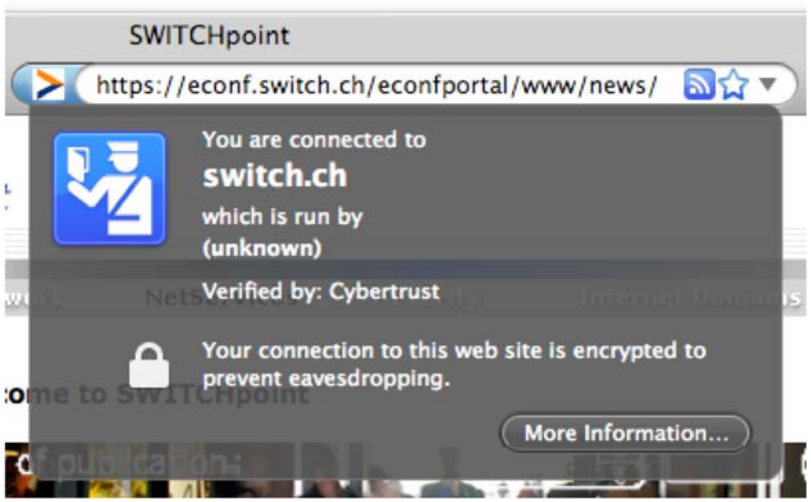
Kaspar Brand
kaspar.brand@switch.ch

Available types of certificates

- Business SSL
  - available with 1-, 2- or 3-year validity
  - for generic SSL/TLS enabled applications: Web servers (HTTP), directory servers (LDAP), Mail servers (IMAP, POP, SMTP), AAI (Shibboleth), RADIUS servers, …
  - certificate extensions etc. almost identical to current SCS/GlobalSign certificates
- Extended Validation (EV) SSL
  - available with 1- or 2-year validity
  - 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)

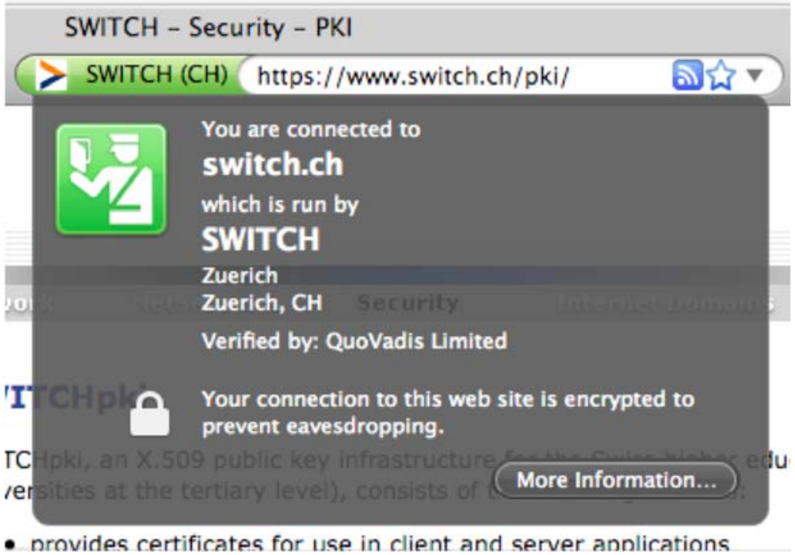
“Standard” (OV) SSL vs. EV SSL

Firefox 3.0



You are connected to
switch.ch
which is run by
(unknown)
Verified by: Cybertrust

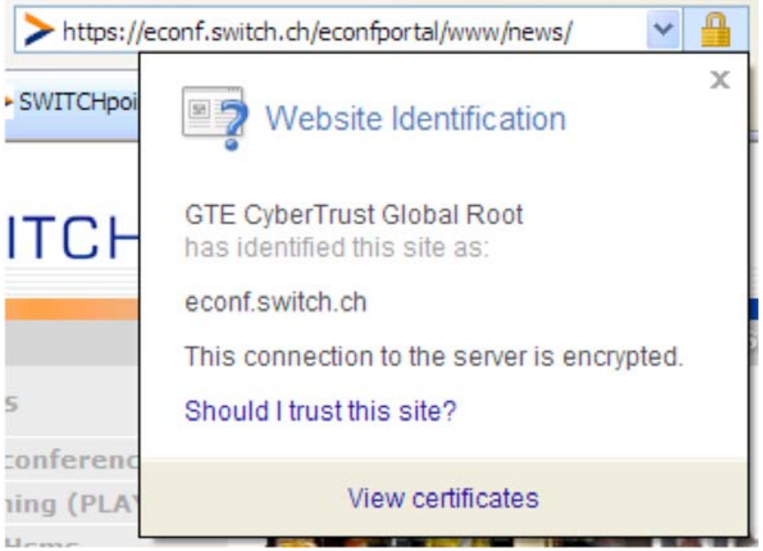
Your connection to this web site is encrypted to prevent eavesdropping.



You are connected to
switch.ch
which is run by
SWITCH
Zuerich
Zuerich, CH
Verified by: QuoVadis Limited

Your connection to this web site is encrypted to prevent eavesdropping.

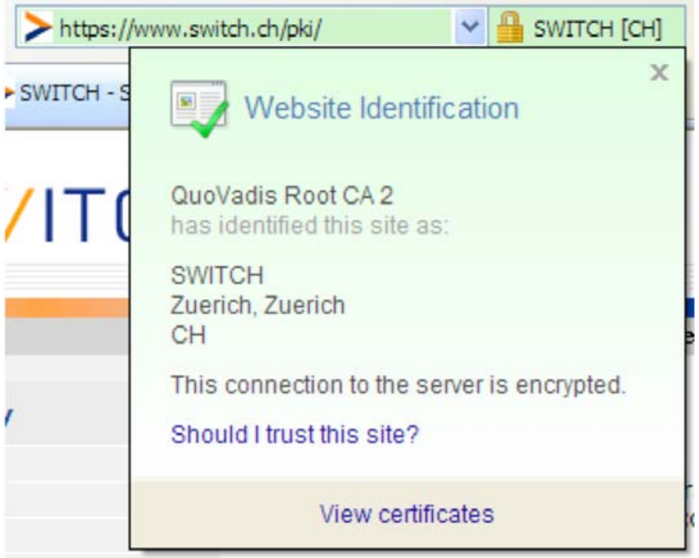
Internet Explorer 7


https://econf.switch.ch/econfportal/www/news/
SWITCHpoi
Website Identification
Should I trust this site?
View certificates

GTE CyberTrust Global Root
has identified this site as:

econf.switch.ch

This connection to the server is encrypted.

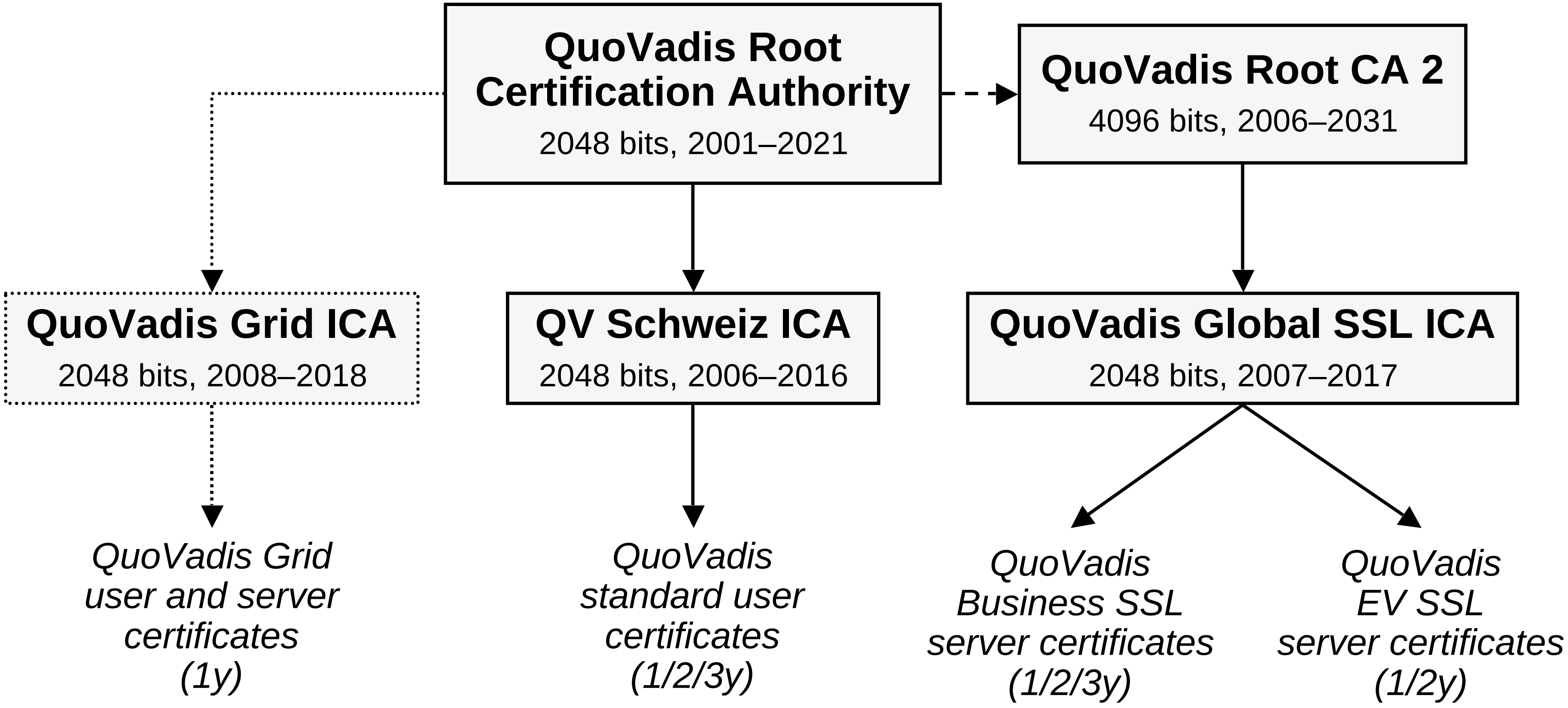


QuoVadis Root CA 2
has identified this site as:

SWITCH
Zuerich, Zuerich
CH

This connection to the server is encrypted.

The QuoVadis CA certificate hierarchy



QuoVadis Root Certification Authority
2048 bits, 2001–2021

QuoVadis Root CA 2
4096 bits, 2006–2031

QuoVadis Grid ICA
2048 bits, 2008–2018

QV Schweiz ICA
2048 bits, 2006–2016

QuoVadis Global SSL ICA
2048 bits, 2007–2017

QuoVadis Grid user and server certificates (1y)

QuoVadis standard user certificates (1/2/3y)

QuoVadis Business SSL server certificates (1/2/3y)

QuoVadis EV SSL server certificates (1/2y)

QuoVadis root certificate preinstallation

- Operating systems
  - Microsoft Windows (XP and later)
  - Apple OS/X (10.2/Jaguar and later) and iPhone OS (2.0 and later)
  - RIM Blackberry OS (4.x and later)
- Applications
  - Mozilla NSS based browsers (Firefox 1.0.2 and later, Seamonkey, Camino, …), mail clients (Thunderbird 1.0.2 and later, Evolution, …)
  - Opera (9.26 and later)
  - KDE/Konqueror (3.5.6 and later)
- Not (yet?) in
  - Java runtime environments (Sun JRE, most notably)
  - Windows Mobile or Symbian based phones

Enrollment procedure for QV certificates

1) Sysadmin generates key pair and creates CSR
2) Sysadmin submits CSR through SWITCH Web form
3) Certificate approver (“admin contact”) receives a challenge e-mail and confirms request
4) SWITCH RA verifies confirmation message
5) EV SSL certificates only: SWITCH RA goes through additional validation steps (as required by the EV Guidelines)
6) SWITCH RA operator issues certificate through Trust/Link SSL
7) Sysadmin receives e-mail message with certificate download instructions

Next steps – timeline

- Paperwork: updated SWITCHpki forms
  - to be published on the SWITCHpki Web site next week
  - still the same set (three 1-page forms: RA agreement, proxy form, DNS domain list)
  - will have to be resubmitted for EV SSL certificate requests (but not for Business SSL)
- QuoVadis Trust/Link SSL 2.0
  - test version for SWITCH available by 15 October (according to QuoVadis' current statements)
  - beta testing for SWITCH customers to start shortly thereafter
  - end of beta test period by 15 November, at the latest