Issuing user certificates with QuoVadis Trust/Link

Options and opportunities

SWITCH

Serving Swiss Universities

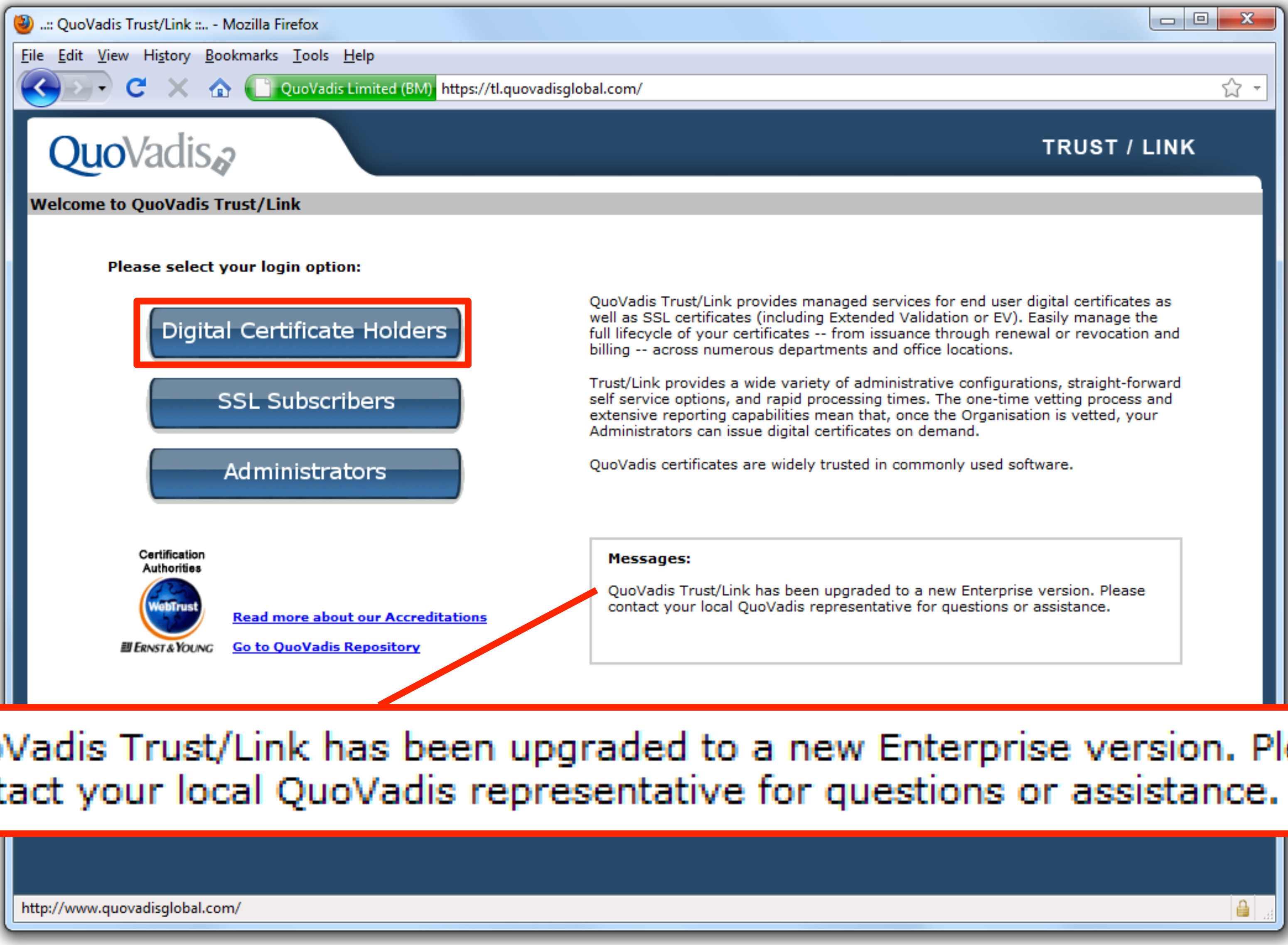
Kaspar Brand
kaspar.brand@switch.ch

Berne, 15th June 2010

User certificates in SWITCHpki

- recurring topic since the days of the AAI-TF-CA (2003)
- the SwissSign-hosted “SWITCH CA” also had a “SWITCH Personal CA” subordinate
  - issuance of user certs limited to RA operators and Grid users
  - SwissSign G1 root certificates not preinstalled in operating systems, browsers etc.
- a survey at the 2nd RA Operator meeting (April 2007) showed only very modest demand for / interest in user certificates
  - based on these results, SWITCH decided to not extend its PKI offering at that time
- but… what about the situation in 2010?

2010-04-26: Trust/Link Enterprise is born



..:: QuoVadis Trust/Link ::.. - Mozilla Firefox
File Edit View History Bookmarks Tools Help
QuoVadis Limited (BM) https://tl.quovadisglobal.com/
QuoVadis
TRUST / LINK
Digital Certificate Holders
SSL Subscribers
Administrators
Certification Authorities
WebTrust
ERNST & YOUNG
Read more about our Accreditations
Go to QuoVadis Repository
http://www.quovadisglobal.com/

Welcome to QuoVadis Trust/Link

Please select your login option:

QuoVadis Trust/Link provides managed services for end user digital certificates as well as SSL certificates (including Extended Validation or EV). Easily manage the full lifecycle of your certificates -- from issuance through renewal or revocation and billing -- across numerous departments and office locations.

Trust/Link provides a wide variety of administrative configurations, straight-forward self service options, and rapid processing times. The one-time vetting process and extensive reporting capabilities mean that, once the Organisation is vetted, your Administrators can issue digital certificates on demand.

QuoVadis certificates are widely trusted in commonly used software.

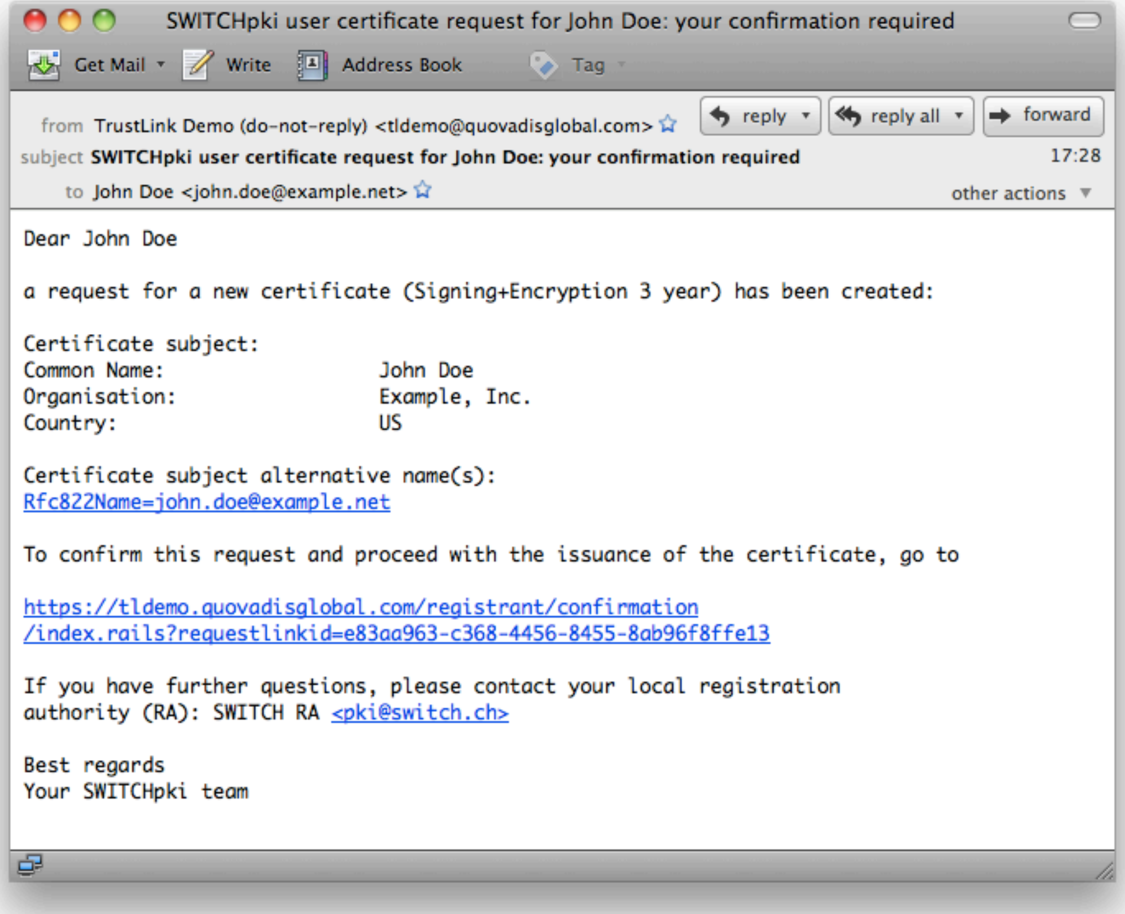
Messages:

QuoVadis Trust/Link has been upgraded to a new Enterprise version. Please contact your local QuoVadis representative for questions or assistance.

QuoVadis Trust/Link has been upgraded to a new Enterprise version. Please contact your local QuoVadis representative for questions or assistance.

How does it look like? Part 1

- From the user's point of view: starts with an e-mail



SWITCHpki user certificate request for John Doe: your confirmation required
Get Mail
Write
Address Book
Tag
reply
reply all
forward
other actions

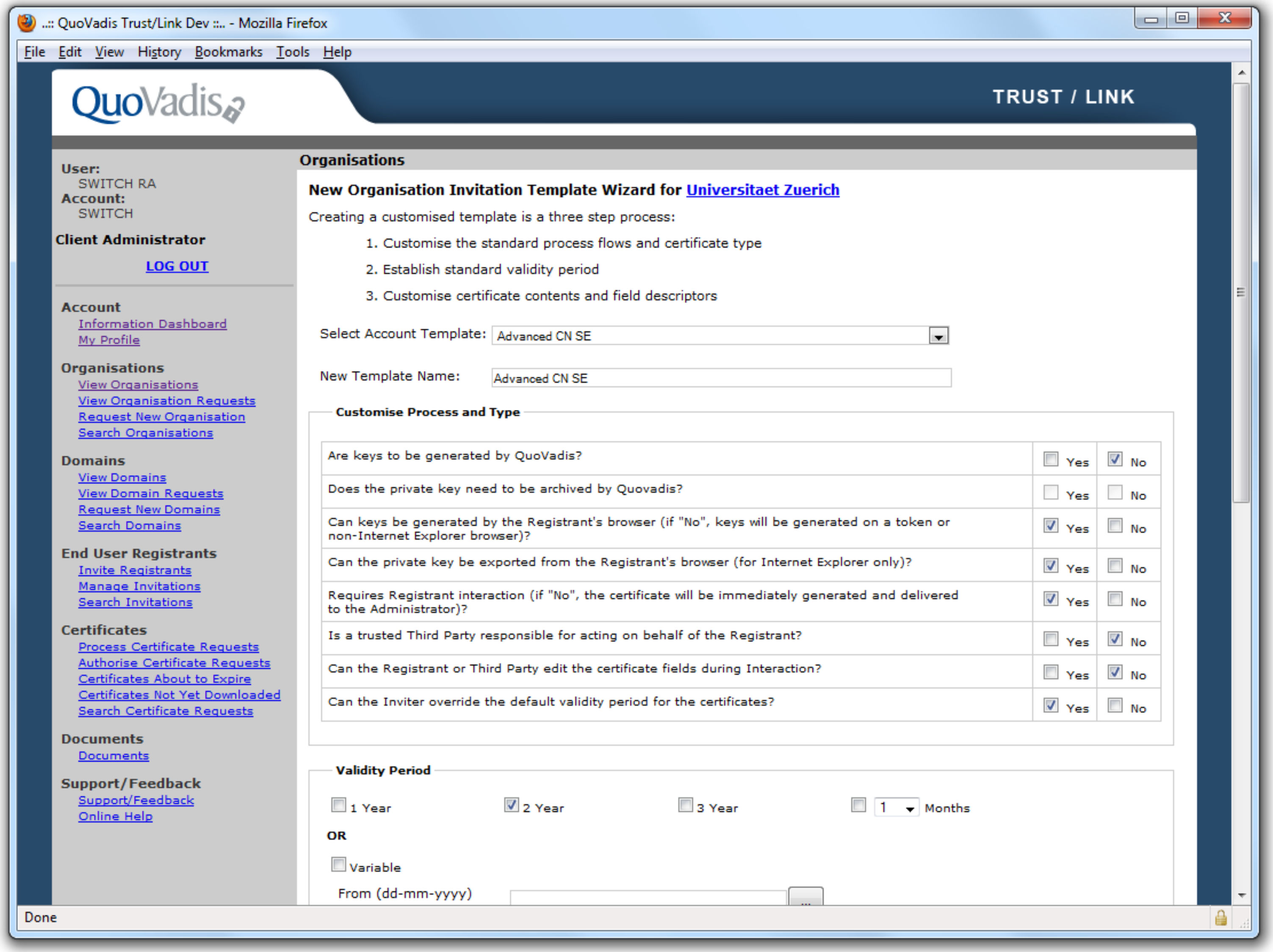
from TrustLink Demo (do-not-reply) <tldemo@quovadisglobal.com>
subject **SWITCHpki user certificate request for John Doe: your confirmation required** 17:28
to John Doe <john.doe@example.net>

```
Dear John Doe

a request for a new certificate (Signing+Encryption 3 year) has been created:

Certificate subject:
Common Name:                  John Doe
Organisation:                 Example, Inc.
Country:                      US

Certificate subject alternative name(s):
Rfc822Name=john.doe@example.net

To confirm this request and proceed with the issuance of the certificate, go to

https://tldemo.quovadisglobal.com/registrant/confirmation
/index.rails?requestlinkid=e83aa963-c368-4456-8455-8ab96f8ffe13

If you have further questions, please contact your local registration
authority (RA): SWITCH RA <pki@switch.ch>

Best regards
Your SWITCHpki team
```

User certificate enrollment

- always triggered by an “invitation”, which is initiated by a Trust/Link administrator (i.e., no unsolicited user requests)
- key generation options:
  - browser based (Firefox, MSIE on Windows, Safari on OS X)
  - supply CSR to Trust/Link admin
- modification of certificate details by the user himself is possible/configurable, but requires an additional approval from a Trust/Link administrator before issuance
- four standard flavors available (with different keyUsage / extendedKeyUsage extensions): *Signing and Encryption, Signing, Encryption, Authentication*

How does it look like? Part 2



Organisations

New Organisation Invitation Template Wizard for Universitaet Zuerich

Creating a customised template is a three step process:

1. Customise the standard process flows and certificate type
2. Establish standard validity period
3. Customise certificate contents and field descriptors

Select Account Template: Advanced CN SE

New Template Name: Advanced CN SE

Customise Process and Type

Are keys to be generated by QuoVadis?	□ Yes	☑ No
Does the private key need to be archived by Quovadis?	□ Yes	□ No
Can keys be generated by the Registrant's browser (if "No", keys will be generated on a token or non-Internet Explorer browser)?	☑ Yes	□ No
Can the private key be exported from the Registrant's browser (for Internet Explorer only)?	☑ Yes	□ No
Requires Registrant interaction (if "No", the certificate will be immediately generated and delivered to the Administrator)?	☑ Yes	□ No
Is a trusted Third Party responsible for acting on behalf of the Registrant?	□ Yes	☑ No
Can the Registrant or Third Party edit the certificate fields during Interaction?	□ Yes	☑ No
Can the Inviter override the default validity period for the certificates?	☑ Yes	□ No

Validity Period

□ 1 Year ☑ 2 Year □ 3 Year □ 1 Months

OR

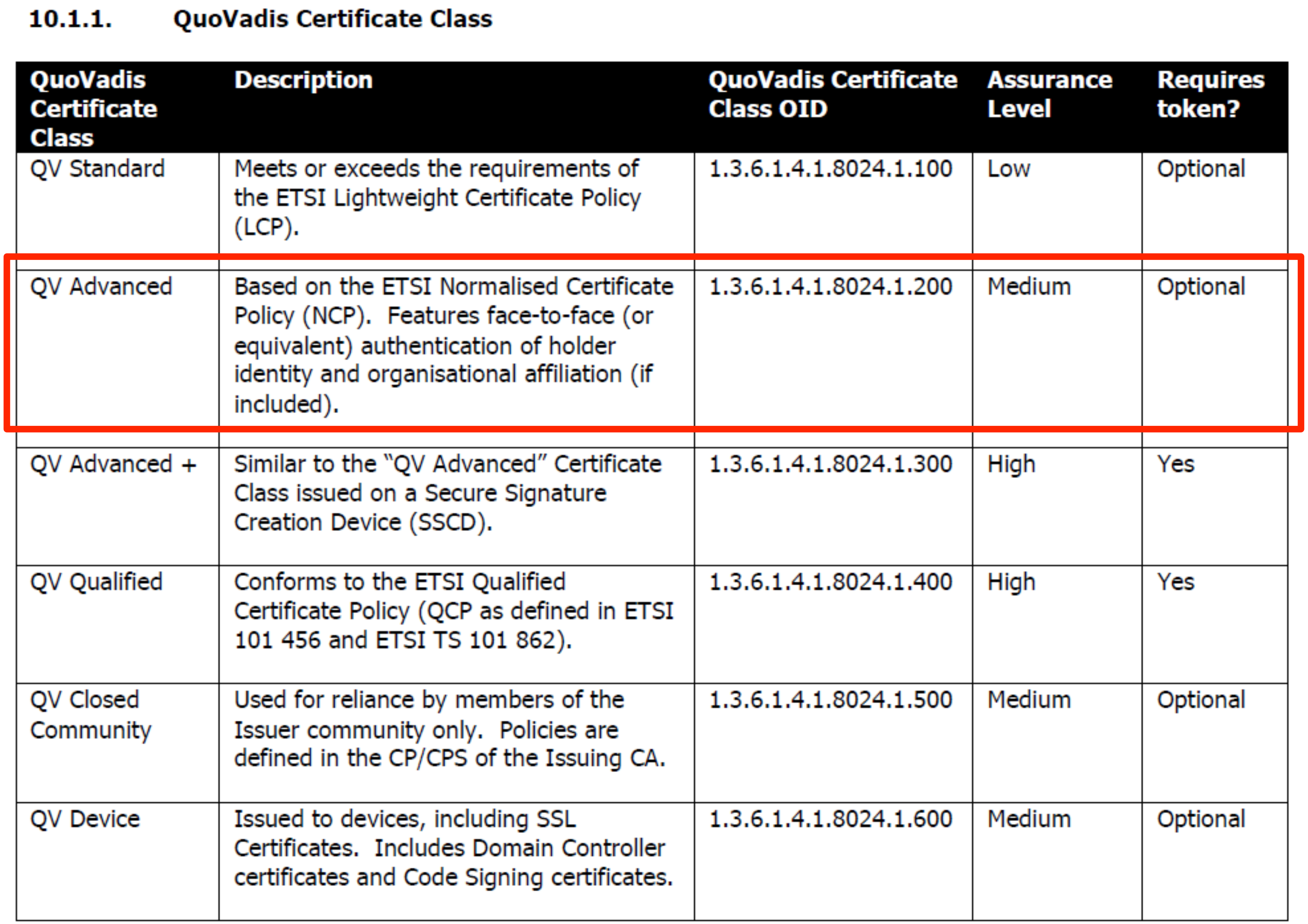
□ Variable

From (dd-mm-yyyy)

Fitting user certificates into SWITCHpki

- no decisions have been taken yet, your opinion wanted
- for RA retail customers, SWITCH RA operators would create invitations
- RA Bulk customers would manage user certs themselves
- you get user certificates with a fully vetted organization name (and no bogus attributes like *OU=Persona Not Validated* etc.), but **TANSTAAFL:**
  - also requires full vetting of the user's identity: high-quality copies of unexpired government-issued ID or passport are prerequisite
  - RA Bulk customers must maintain the document archive themselves
  - neither SWITCH nor QuoVadis will provide support to the (certificate) end users, this job is left to you…

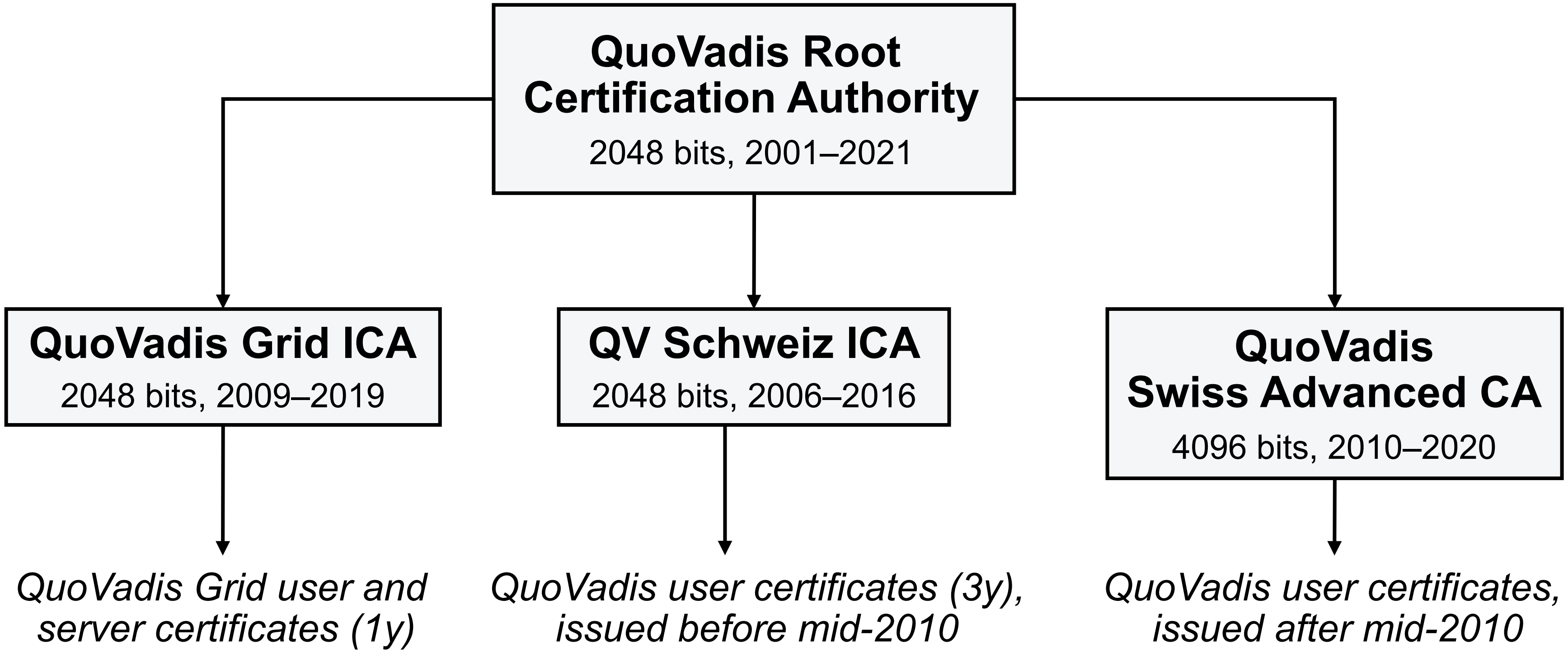
QuoVadis CP/CPS, V4.7



10.1.1. QuoVadis Certificate Class

QuoVadis Certificate Class	Description	QuoVadis Certificate Class OID	Assurance Level	Requires token?
QV Standard	Meets or exceeds the requirements of the ETSI Lightweight Certificate Policy (LCP).	1.3.6.1.4.1.8024.1.100	Low	Optional
QV Advanced	Based on the ETSI Normalised Certificate Policy (NCP). Features face-to-face (or equivalent) authentication of holder identity and organisational affiliation (if included).	1.3.6.1.4.1.8024.1.200	Medium	Optional
QV Advanced +	Similar to the "QV Advanced" Certificate Class issued on a Secure Signature Creation Device (SSCD).	1.3.6.1.4.1.8024.1.300	High	Yes
QV Qualified	Conforms to the ETSI Qualified Certificate Policy (QCP as defined in ETSI 101 456 and ETSI TS 101 862).	1.3.6.1.4.1.8024.1.400	High	Yes
QV Closed Community	Used for reliance by members of the Issuer community only. Policies are defined in the CP/CPS of the Issuing CA.	1.3.6.1.4.1.8024.1.500	Medium	Optional
QV Device	Issued to devices, including SSL Certificates. Includes Domain Controller certificates and Code Signing certificates.	1.3.6.1.4.1.8024.1.600	Medium	Optional

QuoVadis CA hierarchy for user certs



QuoVadis Root Certification Authority
2048 bits, 2001–2021

QuoVadis Grid ICA
2048 bits, 2009–2019

QuoVadis Grid user and server certificates (1y)

QV Schweiz ICA
2048 bits, 2006–2016

QuoVadis user certificates (3y), issued before mid-2010

QuoVadis Swiss Advanced CA
4096 bits, 2010–2020

QuoVadis user certificates, issued after mid-2010

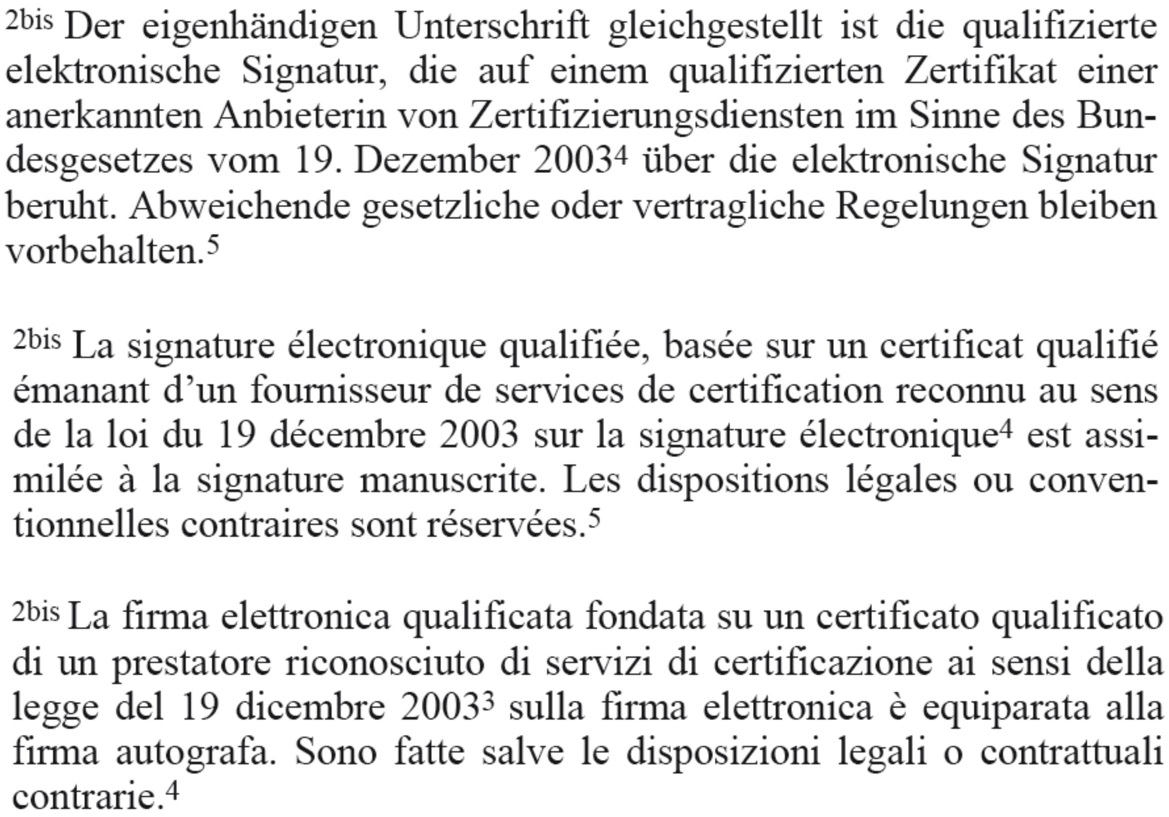
User certs from SWITCHpki: target audience

- SWITCH does not want to compete with existing players in the market for low-assurance user certs
  - for people interested in getting familiar with mail signing or encryption, “free” (i.e., zero-cost) certificates are already available from a couple of CAs
  - if the e-mail address is the only piece in the cert which is “somehow” validated, then that’s often of limited value (*security@uni-xyz.ch* … would you trust a message from this sender, if your mail client shows a proper pen icon?)
- if you need up to a few dozen user certificates per year (for your employees and/or some selected students), then Trust/Link is an elegant solution
- if you consider handing out several hundred / thousands of user certs, then root signing is probably a more attractive path

Caveat emptor

- **Encryption considered harmful:** if you provide your users with certificates for e-mail encryption, don't forget
  - to think about escrowing (nice to have? mandatory?)
  - to educate your users in crypto basics (signing vs. encrypting, examining certificate properties, key management etc.)
  - to consider rules for archiving unencrypted copies
  - to think about worst-case consequences (e.g. decryption key is irretrievably lost)
  - to look into alternatives to message-level encryption
- if you know what you are doing: go ahead!

When interested in things like this…



2bis Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003[4] über die elektronische Signatur beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.[5]

2bis La signature électronique qualifiée, basée sur un certificat qualifié émanant d'un fournisseur de services de certification reconnu au sens de la loi du 19 décembre 2003 sur la signature électronique[4] est assimilée à la signature manuscrite. Les dispositions légales ou conventionnelles contraires sont réservées.[5]

2bis La firma elettronica qualificata fondata su un certificato qualificato di un prestatore riconosciuto di servizi di certificazione ai sensi della legge del 19 dicembre 2003[3] sulla firma elettronica è equiparata alla firma autografa. Sono fatte salve le disposizioni legali o contrattuali contrarie.[4]

[OR/CO Art. 14]

… then listen to the next talk (and get familiar with the SuisseID)