

digicert® + QuoVadis

PSD2

Digital certificates
and related services

Patrick Beckman Lapré

Director Sales & Marketing



1. QuoVadis (quick overview)
2. PSD2:
 1. Overview
 2. Parties involved
 3. Related certificate types
3. Role of the Qualified Trust Service Provider (QTSP)
4. Overview of the request and issuing process of PSD2 related certificates

About QuoVadis (poster)

Topic		Description	Evaluation
	DNA in PKI and digital identities	6 roots in multiple Data Centre (Netherland, Swiss)	+++
	Top (best in class) accreditation		+++
	Ubiquity of trusted roots		+++
	History  	Founded 1999, offices in Switzerland, Germany, Netherlands, Belgium, UK and Bermuda, since January '19 acquired by DigiCert – Co-Owner of CAB International	+++
	Portfolio	360° expertise in managed PKI and electronic signatures and IoT	+++
	Stability	No major incident during the last 18 years – 100% performance given	+++
	Agility	Direct touch to R&D / short (direct) decision cycle – Of the shelf to customized infrastructures	+++
	Conditions	Very low SG&A costs allowing very attractive pricing and Long-term proven and tested reliable products – sunk costs	+++
	Team	Extremely passion belonging over 9 years in average	+++
	Growth and performance	Over 30% growth during last two years over double digit margin	+++
	Clients (Extract)	ABN-AMRO, Rabobank, Achmea, Airbus, Allianz, Bosch, Commerzbank, Daimler, P7S1, Siemens AG, Dutch Lawyer Association (NOVA), PwC, EY, BDO and many more	+++

		Description		Your Benefit
	Reliability & Accreditation	▪ More than 20 Years market expertise ▪ QuoVadis has more accreditations than any other CA, and one of the only EU TSP “qualified” in multiple countries with local operational support. QuoVadis is eIDAS certificated ▪ Ubiquity of trusted Roots for browsers and signing (EU TL & AATL)	➤	» Trust » Reliability » EU trust listed » Best in class accreditation
	Signing Expertise	▪ More than 10 years experience in development and deployment of signing solutions and services – including qualified timestamping services and integration with other platforms / business applications ▪ Focus on remote qualified signing (eIDAS) ▪ Compliance with European and national e-government regulations	➤	» Speed & Expertise » One stop shop » Independent » European
	Flexibility & agility	▪ Modular services composition ▪ Coverage of broad uses cases through standardized solution (configurable) ▪ E.g. one instance and multiple enterprises ▪ Customizing the frontend (branding / look & feel...)	➤	» Fast decisions (No is also answer) » Tailored solutions based on standards » Direct touch to R&D
	Fairness & clarity	▪ Maximum customer effort reduction ▪ Clear responsibility and leadership for project and project management ▪ Long-term proven and tested reliable products ▪ High team retention	➤	» Fair conditions » Contractual flexibility » Harmonization of cash flow (different licensing models are possible)

Customers

digicert® + QuoVadis

Financial services	 
Public & Academic sector	 
Consumer and Health	 
Industrial/ IT / Other	 
Automotive Sector	 

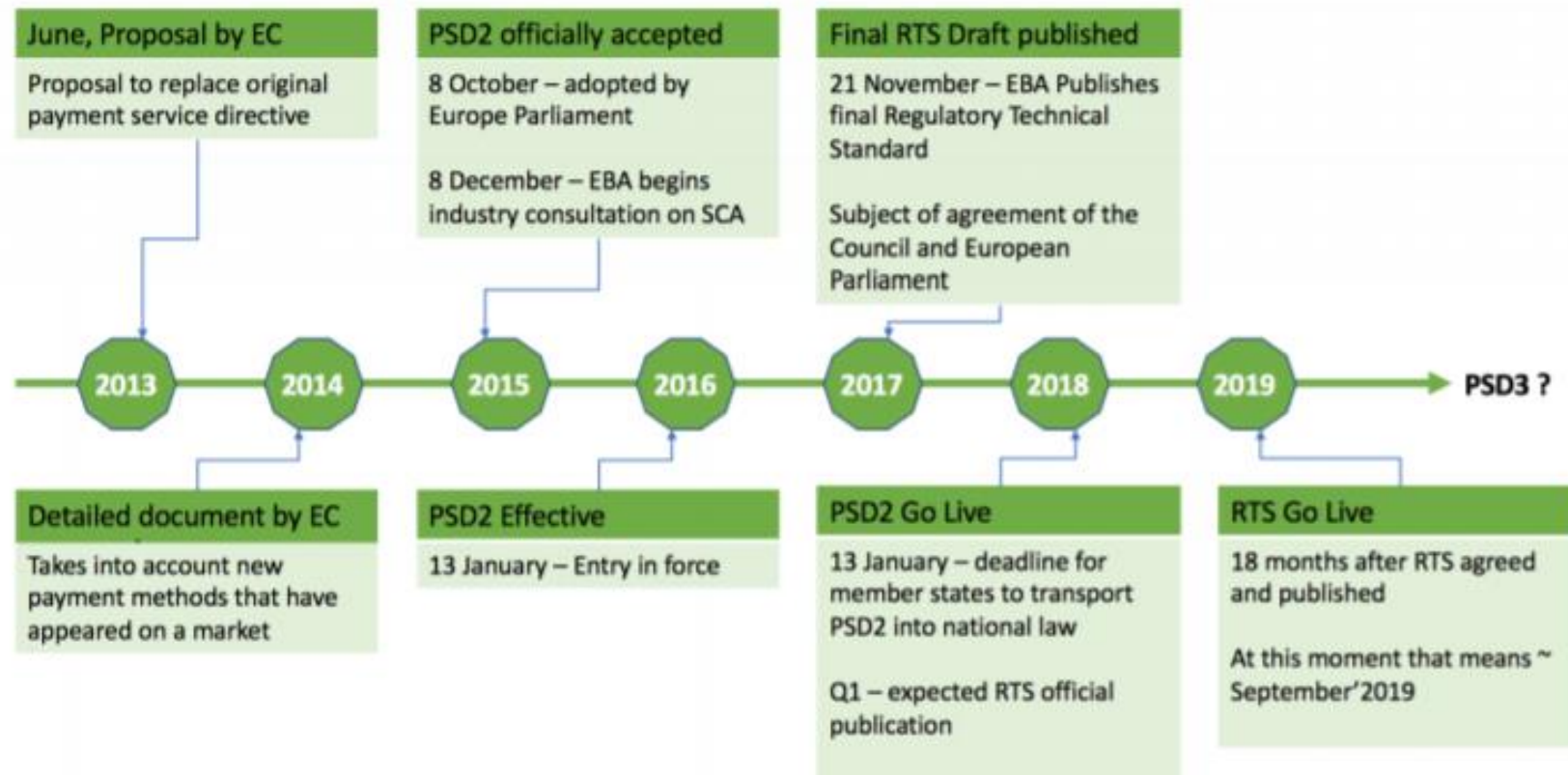
- Huge footprint in all sectors
- Customer in total > 5.000
- Board geographic coverage
- Concentration on Fortune 500, and upscale medium-sized business
- Focus on dedicated partner ships
- 98% Retentions rate

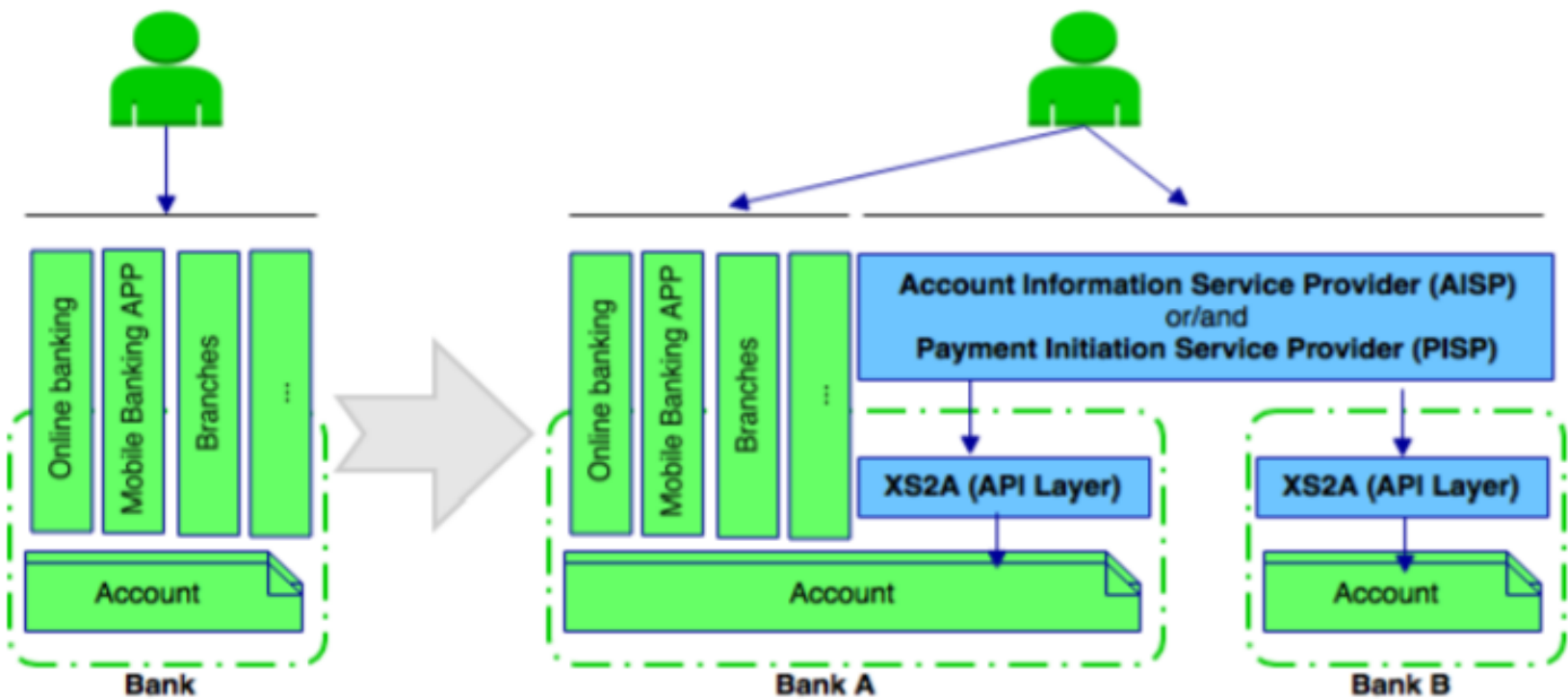


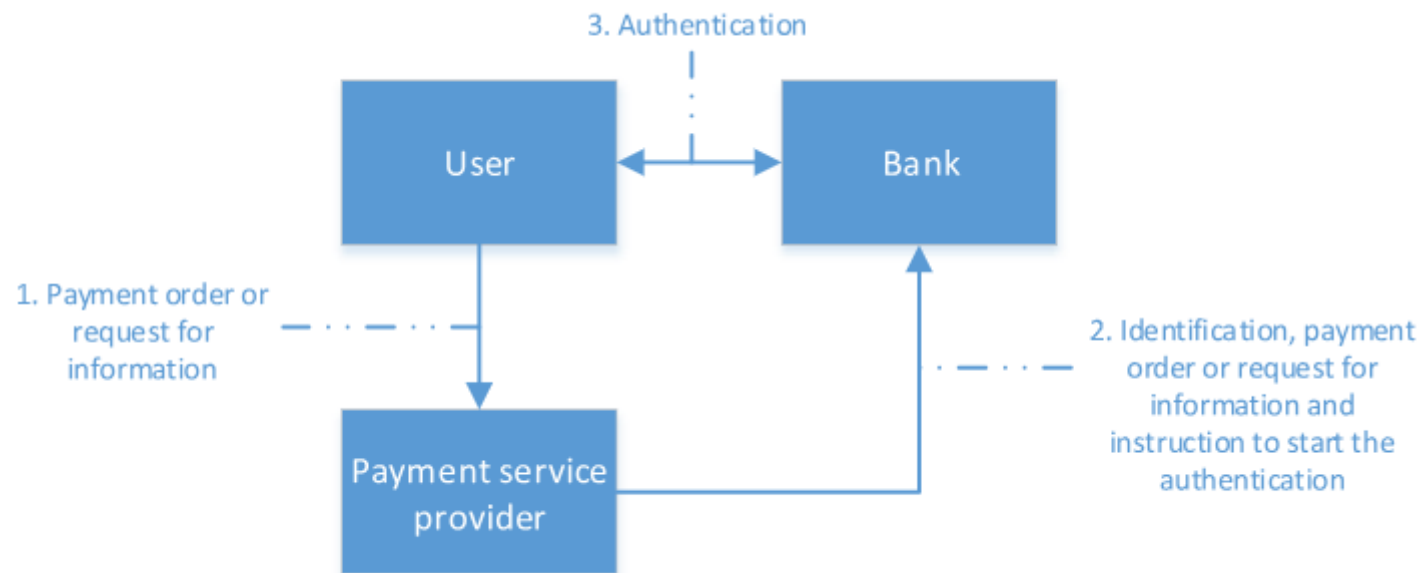
Europese
Commissie

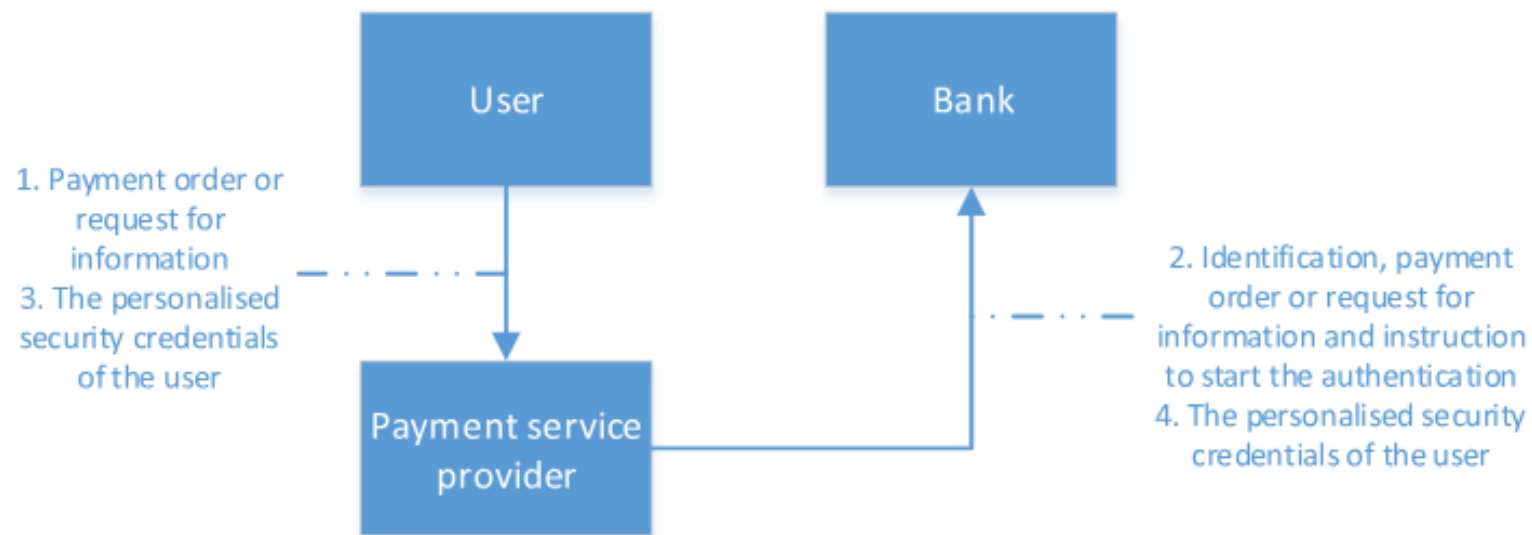












- Bank
- Payment Service Provider (PSP)
 - **PSP** - Payment Service Provider
 - **PSP_AI** - Account Information Service Provider
 - **PSP_AS** - Account Servicing Payment Service Provider
 - **PSP_IC** - Payment Service Provider Issuing Card-based payment instruments
 - **PSP_PI** – Payment Initiation Service Provider
- National Component Authorities (NCA)
 - European Banking Authority (EBA)
 - Open Banking Europe - PRETA

- Qualified **Trust** Service Provider (QTSP)



- **Trust** is based on three pillars:
 - ✓ Original information vetting
 - ✓ Security of key material
 - ✓ underlying legislation

PDS2 related certificate types:

➤ Qualified Website Authentication Certificate (**QWAC**)

- Guarantees the identity of the organisation
- Used for securing the transport layer (Transport Layer Security - TLS)
- Contains a QC statement, QWAC and EV OID
- (= European regulated Extended Validation (EV) SSL)



EV SSL	QWAC
Face-to-face identification authorized representative - optional	Face-to-face identification authorized representative - mandatory/required
Regulations based on CA/B forum requirements	Regulation based on European law (which refers to CA/B forum).



PDS2 related certificate types:

➤ Qualified eSeal Certificate (**QeSealC**)

- 'Legal person representing an organisation'
- Used for signing the data transported
- Guarantees the identity and integrity of the signed data
- Qualified Signature Creation Device (**QSCD**)
 - USB token, smart card or Hardware Security Module (HSM)



Challenges regarding the issuance of PDS2 related certificates:

- PDS2 requires additional/different content in the certificate:
 - PSP role(s)
 - **PSP** - Payment Service Provider
 - **PSP_AI** - Account Information Service Provider
 - **PSP_AS** - Account Servicing Payment Service Provider
 - **PSP_IC** - Payment Service Provider Issuing Card-based payment instruments
 - **PSP_PI** – Payment Initiation Service Provider
 - OrgIdentifier
 - ...
- Other:
 - Local NCA involvement at issuance and revocation of a certificate
 - Role of EBA/PRETA



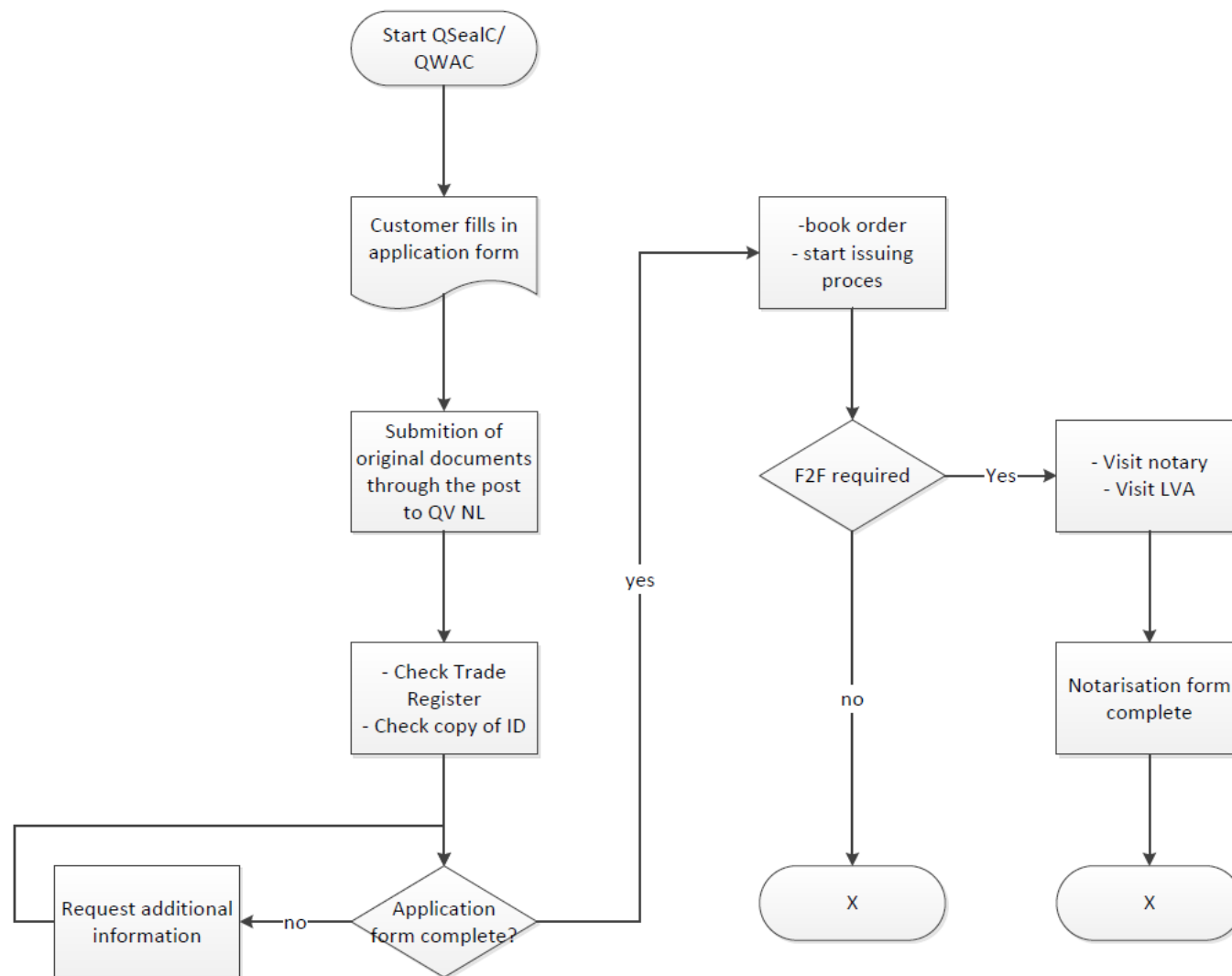
Challenges regarding the issuance of PDS2 related certificates:

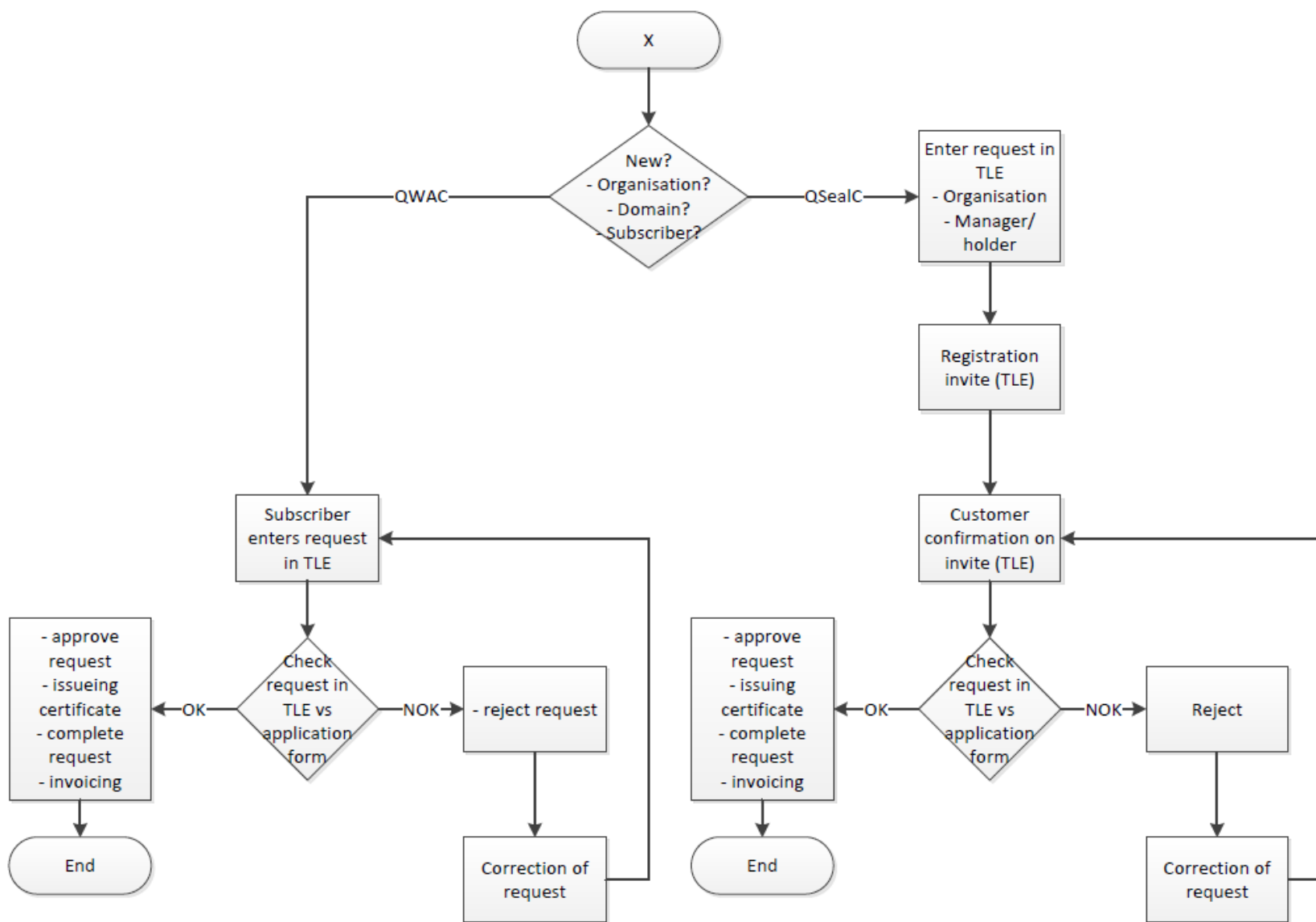
➤ Other:

- QeSealC on QSCD vs QeSealC non QSCD
- Usage of a Hardware Security Module (HSM) for high volume signing capacity



Request flow





Data needed for QWAC

- Application form

Includes:

- o Content certificate:
 - Common Name
 - Organisation Name
 - Name Trade Register
 - Number in Trade Register
 - Location
 - State
 - Country
- o Additional data:
 - Validity (2 year (= default) or 1 year)
 - Main phone number
 - Visiting Address
 - ZIP code + Country
- o Certificate Manager:
 - Surname (as on passport/ID card)
 - Given name (as on passport/ID card)
 - Date of Birth, Town and Country
 - Nationality
 - Personal company e-mail address
 - Personal company phone number
 - First secret Question
 - Answer to first secret question
 - Second secret Question
 - Answer to second secret question
- o Authorized Representative (as mentioned in the trade register):
 - Surname (as on passport/ID card)
 - Given name (as on passport/ID card)
 - Type of identification document (passport or ID card)
 - ID document valid until

Qualified eSeal:

- Application form

Includes:

- Content certificate:
 - Common Name
 - Organisation Name
 - Name Trade Register
 - Number in Trade Register
 - Location
 - State
 - Country
 - (PDS2 specific) – PSP identifier/code
- Additional data:
 - Validity (2 year (= default) or 1 year)
 - Main phone number
 - Visiting Address
 - ZIP code + Country
- Certificate Manager:
 - Surname (as on passport/ID card)
 - Given name (as on passport/ID card)
 - Date of Birth, Town and Country
 - Nationality
 - Personal company e-mail address
 - Personal company phone number
 - First secret Question
 - Answer to first secret question
 - Second secret Question
 - Answer to second secret question
- Authorized Representative (as mentiond in the trade register):
 - Surname (as on passport/ID card)
 - Given name (as on passport/ID card)
 - Type of identification document (passport or ID card)
 - ID document valid until

Change process of a certificate is depending of the situation.

- Renewal of a valid/existing certificate
- Change in case of changed situation
- Change in relation to a revocation

Revocation process of a certificate

- At the moment a valid certificate isn't representing the actual situation the QTSP is required to revoke the certificate(s) within **24** hrs.

- **Who can initiate a revocation?**
 - Certificate Requestor/Holder or Certificate Manager
 - Local NCA in case of a withdrawn of a role
 - Supervisory Body (in NL – Agentschap Telecom)
 - QTSP



digicert® + QuoVadis

Contact info:

Office:

+31 (0)30 2324320

Mobile:

+31 (0)6 12853576

E-mail:

p.beckmanlapre@quovadisglobal.com