QuoVadis

PKI Disclosure Statement

OIDs:	1.3.6.1.4.1.8024.0.1
	1.3.6.1.4.1.8024.0.2
	1.3.6.1.4.1.8024.0.3
Effective Date:	5 July, 2021
Version:	1.15

Important Notice about this Document

This document is the PKI Disclosure Statement (PDS) of QuoVadis Limited (QuoVadis), a company of DigiCert, Inc. The purpose of this document is to summarise the key points of the QuoVadis CP/CPS for the benefit of Subscribers and Relying Parties.

This document does not substitute or replace the Certificate Policy/Certification Practice Statement (CP/CPS) under which Certificates issued by QuoVadis are issued. This PDS relates to the following CP/CPS documents:

- CP/CPS for QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3
- CP/CPS for QuoVadis Root CA 2 and QuoVadis Root CA 2 G3

You must read the relevant CP/CPS at https://www.quovadisglobal.com/repository before you apply for or rely on a Certificate issued by QuoVadis.

This document is not intended to create contractual relationships between QuoVadis and any other person. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business.

This version of the PDS has been approved for use by the QuoVadis Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA. The date on which this version of the PDS becomes effective is indicated on this document.

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement
QuoVadis PMA	15 June 2017	1.1	Based on ETSI TS319 411 model disclosure statement and eIDAS regulation
QuoVadis PMA	13 September 2017	1.2	Updates for submission of complaints.
QuoVadis PMA	20 August 2018	1.3	Updates for Qualified Website Authentication Certificates and link to Privacy Notice.
QuoVadis PMA	30 august 2018	1.4	Update for Qualified website authentication certificates information
QuoVadis PMA	7 December 2018	1.5	Updates to include changes for EU Qualified certs and itsme Sign Issuing CA. More explicit reference to the BR Domain Vetting methods.
QuoVadis PMA	5 June 2019	1.6	Updates for where QSCD managed on behalf of Subscriber by QuoVadis.
QuoVadis PMA	20 June 2019	1.7	Updates for PSD2 QCP-w-psd2 and QSealC.
QuoVadis PMA	31 March 2020	1.8	Changes to comply with Mozilla Root Store Policy v2.7, CA/B Forum Ballot SC25, revised Subscriber Agreement and Terms of Use, and new Swiss policies. Changes to reflect policies and practices adopted from, and editorial conformity with, DigiCert where applicable.
QuoVadis PMA	25 August 2020	1.9	Updates to certificate profiles in coordination with CP/CPS.
QuoVadis PMA	30 September 2020	1.10	Updates in coordination with CP/CPS.
QuoVadis PMA	22 March 2021	1.11	Updates in coordination with CP/CPS, expiration of QuoVadis Root Certification Authority.
QuoVadis PMA	28 June 2021	1.12	Minor updates in coordination with CP/CPS.
QuoVadis PMA	6 December 2021	1.13	Updates for ETSI TS 119 461, identity proofing.
QuoVadis PMA	20 December 2021	1.14	Clarification of identity proofing methods.
QuoVadis PMA	5 July 2022	1.15	Minor updates in coordination with CP/CPS.

TABLE OF CONTENTS

1. CA CONTACT INFO

Website: https://www.quovadisglobal.com/
Repository: https://www.quovadisglobal.com/repository
Customer complaints email: qvcomplaints@digicert.com

Bermuda QuoVadis Limited Washington Mall 3F 7 Reid Street Hamilton HM-11 Bermuda Phone: +1-441-278-2800	**Belgium** DigiCert Europe Belgium BV (previously QuoVadis Trustlink BVBA) Schaliënhoevedreef 20T 2800 Mechelen Belgium Phone: +32 15-79-65-21
Germany QuoVadis Trustlink Deutschland GmbH Ismaninger Str. 52 D-81675 München Germany Phone: +49-89-540-42-45-42	**Netherlands** QuoVadis Trustlink BV Nevelgaarde 56 noord 3436 ZZ Nieuwegein The Netherlands Phone: +31 (0) 30 232-4320
Switzerland QuoVadis Trustlink Schweiz AG Poststrasse 17, Postfach 9001 St. Gallen Switzerland Phone: +41 71-228-98-00	**United Kingdom** QuoVadis Online Limited 2 Harbour Exchange Square London, E14 9GE United Kingdom Phone: +44 (0) 333-666-2000

1.1. REVOCATION REPORTING

QuoVadis provides additional information for entities requiring assistance with revocation or an investigative report at https://www.quovadisglobal.com/certificate-revocation. *See also* Section 4.9.2 of the CP/CPS.

For anyone listed in Section 4.9.2 of the relevant CP/CPS and the CA/Browser Baseline Requirements that requires assistance with revocation or investigative reports, QuoVadis provides this page for reporting and submitting requests with all of the necessary information as outlined in Section 4.9:
https://problemreport.digicert.com/

If the problem reporting page is unavailable, there is a system outage, or you believe our findings are incorrect please contact revoke@digicert.com.

Entities submitting Certificate revocation requests must explain the reason for requesting revocation. QuoVadis or an RA will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. QuoVadis will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorised representative of the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Affiliated Organisation, QuoVadis or an RA will investigate the alleged basis for the revocation request prior to taking action. *See also* Section 4.9.1 and 4.9.3 of the CP/CPS.

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI an Issuing CA can only issue Certificates with approved Certificate Profiles. The procedures for Subscriber registration and validation are described below for each type of Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described below or in the CP/CPS may be drawn up under contract for individual customers. Please refer to the CP/CPS for the full details.

Please note that where the term "Qualified Certificate" is used in this document it is consistent with the definition of "Qualified Certificate" in ETSI EN 319 411-2 and Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation"). QuoVadis Qualified CAs are listed on the EU Trusted List (EUTL) for the Netherlands and for Belgium.

In the case of Qualified Certificates, where QuoVadis manages the keys on behalf of the Subscriber, QuoVadis shall require:

- where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures are only created by the QSCD;
- in the case of natural persons, the Subscribers' private key is maintained and used under their sole control and used only for electronic signatures; and
- in the case of legal persons, the private key is maintained and used under their control and used only for electronic seals.

2.1. QUOVADIS CERTIFICATE CLASSES

Certificate Class	**Description**	**Policy OID**	**Assurance Level**	**Requires token?**
QV Standard	Based on the ETSI Lightweight Certificate Policy (LCP), which has the policy identifier OID 0.4.0.2042.1.3	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.100 ETSI policy identifier OID: 0.4.0.2042.1.3 (optional)	Low	Optional
QV Advanced	Based on the ETSI Normalised Certificate Policy (NCP), which has the OID 0.4.0.2042.1.1. Features face-to-face (or equivalent) authentication of holder identity and organisational affiliation (if included).	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.200 ETSI policy identifier OID: 0.4.0.2042.1.1 (optional)	Medium	Optional
QV Advanced +	Similar to "QV Advanced" issued on an SSCD. Based on the ETSI Normalised Certificate Policy requiring an SSCD (NCP+), which has the OID 0.4.0.2042.1.2 Includes Swiss Regulated Certificates.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300 ETSI policy identifier OID: 0.4.0.2042.1.2 (optional)	High	Yes Adobe AATL Approved

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
QV Qualified	QuoVadis Qualified Certificate on a QSCD	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.400 ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)	High	Yes Adobe AATL Approved
	QuoVadis Qualified Certificate on a QSCD, where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.410	High	Yes
	Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n-qscd), with the OID 0.4.0.194112.1.2 EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the OID 0.4.0.194112.1.3	ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)		Adobe AATL Approved
	QuoVadis Qualified Certificate not on a QSCD. Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	QuoVadis Qualified Certificate not on a QSCD, where the device is managed by a QTSP. Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.460 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
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 Time-stamp Certificates.	1.3.6.1.4.1.8024.1.600	Medium	Optional

QuoVadis provides test certificates for all types of Certificates.

2.2. KEY USAGE AND ARCHIVE

Different QuoVadis Certificate Profiles may be issued with different key usages, and be eligible for Key Escrow, according to the following table:

QuoVadis Certificate Type	**Key Usage/ Extended Key Usage Options**	**Applicability to QuoVadis Certificate Classes**			
		QV Standard	**QV Advanced**	**QV Advanced +**	**QV Qualified**
Signing and Encryption	**Key Usage** digitalSignature nonRepudiation keyEncipherment keyAgreement **Extended Key Usage** smartcardlogon clientAuth emailProtection documentSigning enrolmentAgent	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow not permitted)	Not Allowed
Signing	**Key Usage** digitalSignature nonRepudiation **Extended Key Usage** smartcardlogon clientAuth emailProtection documentSigning enrolmentAgent	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)
Encryption	**Key Usage** keyEncipherment keyAgreement **Extended Key Usage** emailProtection	Allowed (Escrow permitted)	Allowed (Escrow permitted)	Allowed (Escrow not permitted)	Not Allowed
Authentication	**Key Usage** digitalSignature **Extended Key Usage** smartcardlogon clientAuth enrolmentAgent	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Not Allowed

2.3. IDENTITY AUTHENTICATION

If the Subject is an Organisation (legal person), evidence shall be provided of:

i) Full name of the legal person;

ii) Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name; and

iii) When applicable, the association between the legal person and any other organisational entity identified in association with this legal person that would appear in the Organisation attribute of the Certificate, consistent with the national or other applicable identification practices.

If the Subject is a natural person, evidence shall be provided to deliver unique identification of the Applicant, including:

i) Full name (including surname and given names consistent with applicable law and national identification practices); and

ii) Date and place of birth,or reference to at least one nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Subject is a natural person identified in association with a legal person, additional evidence shall be provided of:

i) Full name and legal status of the associated organisational entity;

ii) Any relevant existing registration information (e.g. company registration) of the organisational entity; and

iii) Evidence that the Subject is affiliated with the organisational entity which may include reference to an attestation or a trusted register. Attestations may be made by directors, executives, board members, or a natural person with authorisation duly delegated from another natural person in an authorised role.

Delegated administrators at Enterprise RAs may assert an Applicant's affiliation with the organisational entity using the QuoVadis Certificate Management System.

By requesting a QuoVadis Certificate, an Applicant accepts to undertake one of the following identity proofing methods and the related terms and conditions. QuoVadis may provide alternative identity verification methods available to the relevant Certificate Class:

- Physical presence;
- Remote Identity Verification which provides equivalent assurance in terms of reliability to the physical presence;
- Reliance on an Electronic Signature; and/or
- Video verification.

See also Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Where required by a Certificate Class, QuoVadis only allows use of specific identity proofing means following approval of the method by the relevant Conformity Assessment Body and/or Supervisory Body. QuoVadis supports four levels of Remote Identity Verification:

Level	**Description**
RIV1	Base RIV plus manual review in defined cases (e.g, fraud risk, changes made by RA)
RIV2	Base RIV plus manual review in all cases
RIV3	Base RIV plus NFC Authentication with manual review in defined cases (e.g, fraud risk, changes made by RA)
RIV4	Base RIV plus NFC Authentication with manual review in all cases

Base RIV includes OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options include read of eMRTD data, Passive Authentication, and Active Authentication.

2.4. CERTIFICATE CLASSES

2.4.1. QV Standard

Purpose
Standard Certificates provide flexibility for a range of uses appropriate to their reliance value including S/MIME, electronic signatures, authentication, and encryption.
Registration Process
Validation procedures for QuoVadis Standard Certificates collect either direct evidence or an attestation from an appropriate and authorised source of the identity (such as name and organisational affiliation) and other specific attributes of the Subject. Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. Identity proofing may be conducted via enterprise records, physical presence, Remote Identity Verification (RIV1-4), reliance on electronic signature, or video verification.

2.4.2. QV Advanced

Purpose
QV Advanced Certificates provide reliable verification of the Subject's identity and may be used for a broad range of applications including Digital Signature, encryption, and authentication.
Registration Process
Validation procedures for Advanced Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1. Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on electronic signature. If the Subscriber is a natural person who is identified in association with a legal person (organisational entity), additional evidence shall be provided of: • Full name and legal status of the associated legal person; • Any relevant existing registration information (e.g. company registration) of the associated legal person; and • Evidence that the Subscriber is affiliated with the legal person. If the Subscriber is a legal person (organisational entity), evidence shall be provided of: • Full name of the legal person; and • Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name. If the Subscriber is a device or system operated by or on behalf of a legal person, evidence shall be provided of: • identifier of the device by which it may be referenced (e.g. Internet domain name);

- full name of the organisational entity;
- a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

2.4.3. QV Advanced +

Purpose
QuoVadis Advanced+ Certificates are used for the same purposes as Advanced Certificates, with the only difference being that they are issued on a Secure Cryptographic Device either held by the Subscriber or managed by QuoVadis. The QuoVadis Advanced+ Certificate Class is trusted in the Adobe Approved Trust List (AATL). Swiss Regulated Certificates issued under the Swiss Federal signature law (ZertES) are included in the Advanced+ class.
Registration Process
QuoVadis Advanced+ Certificates are based on with the Normalised Certificate Policy (NCP+) described in ETSI EN 319 411-1. The registration process and identity vetting process for QV Advanced + Certificates is the same as QV Advanced Certificates. Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification, or reliance on electronic signature. AATL Certificates may use RIV1 or higher, ETSI Certificates may use RIV4 for NFC with RIV2 as a fallback option if NFC is not available. QuoVadis Advanced+ Certificates must be issued on a Secure Cryptographic Device and adhere to the following requirements: • Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA or RA; • User activation data is securely prepared and distributed separately from the Secure Cryptographic Device; • If keys are generated under the Subscriber's control, they are generated within the Secure Cryptographic Device used for signing or decrypting; • The Subscriber's Private Key can be maintained under the subject's sole control; and • Only use the Subscriber's Private Key for signing or decrypting with the Secure Cryptographic Device.

2.4.3.1. Swiss Regulated Certificate issued to a Natural Person

Purpose
Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ Certificate Class. They are issued out of Swiss Regulated CAs and have the notice text "regulated certificate" in the CertificatePolicies user notice.
Registration Process
Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates. For the issuance and life cycle management of Swiss Regulated Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES Qualified Certificate.

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.

Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS 140-2 level 3 or EAL 4 standards. This Hardware is either a USB-token handed out to clients or a HSM located in a QuoVadis datacentre. The level of assurance using a HSM aims to be the same as achieved by a stand-alone SSCD. Access by the Subscriber to the keys is protected using multifactor authentication.

Swiss Regulated Certificates have a maximum validity of three years.

2.4.3.2. Swiss Regulated Certificate issued to a Legal Person (Company Seal)

Purpose
Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QV Advanced+ Certificate Class. Swiss Regulated Certificates are issued out of the "QuoVadis Swiss Regulated CAs" and have the notice text "regulated certificate" in the CertificatePolicies user notice.
Registration Process
Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates. Subjects may include an Organisation (legal person). Only methods approved for ZertES may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES. Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS 140-2 level 3 or EAL 4 standards. This Hardware is either a USB-token handed out to clients or an HSM located in a QuoVadis datacentre. The level of assurance using an HSM aims to be the same as achieved by a stand-alone SSCD. Access by the Subscriber to the keys is protected using multifactor authentication. Swiss Regulated Certificates have a maximum validity of three years.

2.4.4. QV Qualified

2.4.4.1. eIDAS Qualified Certificate issued to a Natural Person on a QSCD

Purpose
The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation. These Certificates meet the relevant ETSI "Policy for EU

qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd).

Swiss Qualified Certificates issued under the Swiss Federal signature law (ZertES) also meet this ETSI policy QCP-n- qscd. These Swiss Qualified Certificates are issued only to natural persons out of the "QuoVadis Swiss Regulated CA G1" and have the notice text "qualified certificate" in the CertificatePolicies user notice.
The content of these Certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

Registration Process

Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd). QuoVadis recommends that QCP-n-qcsd certificates are used only for electronic signatures.

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. Only methods approved for eIDAS Qualified Certificates may be used. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.

These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

2.4.4.2. eIDAS Qualified Certificate issued to a Natural Person

Purpose

The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.

This type of QuoVadis Qualified Certificates does not use a QSCD for the protection of the private key. The content of these Certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

Registration Process

The identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for the "Policy for EU qualified certificate issued to a natural person" (QCP-n). The registration process for these certificates is the same as for the QCP-n-qcsd Certificates. The only difference is that these QCP-n certificates do not use a QSCD for the protection of the private key.

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. Only methods approved for eIDAS Qualified Certificates may be used. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS.

Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.

The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

2.4.4.3. eIDAS Qualified Certificate issued to a Legal Person on a QSCD

Purpose

The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

This type of QuoVadis Qualified Certificates uses a QSCD for the protection of the private key.

These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd). QuoVadis recommends that QCP-l-qscd certificates are used only for electronic seals.

The content of these Certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

Registration Process

Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd).

Subjects may include an Organisation (legal person). Only methods approved for eIDAS Qualified Certificates may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS.

Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.

These Certificates require a Qualified Signature Creation Device (QSCD) that meets the requirements laid down in annex II of Regulation (EU) N° 910/2014. In some cases, QuoVadis generates and manages private keys on behalf of the Subscriber and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies.

The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

For PSD2 Certificates, additional steps verify specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA.

2.4.4.4. eIDAS Qualified Certificate issued to a Legal Person

Purpose

The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person" (QCP-l). QuoVadis recommends that QCP-l certificates are used only for electronic seals. The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

Registration Process

Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person" (QCP-l).

The registration process for these Certificates is the same as for the QCP-l-qcsd Certificates. The only difference is that these QCP-l certificates do not use a QSCD for the protection of the private key.

Subjects may include an Organisation (legal person). Only methods approved for eIDAS Qualified Certificates may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3.

Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.

The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

For PSD2 Certificates, additional steps verify specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA.

2.4.4.5. Swiss Qualified Certificate

Purpose

QV Swiss Qualified Certificates are Qualified personal certificates according to the Swiss Federal signature law (ZertES). They are issued out of the "QuoVadis Swiss Regulated CAs" and have the notice text "qualified certificate" in the Certificate Policies user notice. QV Swiss Qualified Certificates are used to sign documents electronically. The Digital Signature is tamperproof and legally equivalent to a handwritten signature.

Registration Process

QV Swiss Qualified Certificates are issued in accordance with the ZertES requirements using various QuoVadis Signing Services designed for this type of Certificate. The guidelines in TAV-ZERTES apply to QV Swiss Qualified Certificates.

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Only Remote Identity Verification means approved according to ZertES may be used.

Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on Qualified Electronic Signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.

Private Keys for QV Swiss Qualified Certificates are generated and stored on an HSM Hardware Security Module or USB token that meets the ZertES requirements, FIPS 140-2, level 3 or EAL 4 standards. HSMs for QuoVadis Signing Services are located in QuoVadis datacentres. Access by the Subscriber to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone SSCD.

QV Swiss Qualified Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour.

2.4.4.6. QuoVadis Qualified Website Authentication (QCP-w)

Purpose

ETSI EN 319 411-2 defines "QCP-w" as the "policy for EU Qualified website certificate issued to a natural or a legal person and linking the website to that person". QuoVadis policy is that QuoVadis Qualified Website Authentication (QCP-w) Certificates will only be issued to legal persons and not natural persons.

QuoVadis QCP-w Certificates will be issued under the requirements of ETSI EN 319 411-2 aim to support website authentication based on a Qualified defined in articles 3 (38) and 45 of the eIDAS Regulation.

QCP-w Certificates issued under these requirements endorse the requirement of EV Certificates whose purpose is specified in clause 5.5 of ETSI EN 319 411-1 [2]. In addition, EU Qualified Certificates issued under this policy may be used to provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website as specified in the eIDAS Regulation. The certificate profile below is designed in accordance with:

- EV Guidelines;
- ETSI EN 319 411-2;
- ETSI EN 319 412-4: Certificate profile for web site certificate;
- ETSI EN 319 412-5; and
- Where relevant for PSD2, ETSI TS 119 495

Registration Process

The verification requirements for a QuoVadis Qualified Website Authentication Certificates (QCP-w) are consistent with the vetting requirements for a QuoVadis EV SSL Certificate (described in the QuoVadis Root CA2 CP/CPS), with the following additional verification:

QuoVadis Qualified Website Authentication (QCP-w) Certificates are only issued to legal persons and not natural persons.

Identity proofing of the authorised representative of the legal person may be conducted via physical presence, Remote Identity Verification (RIV4 only), or reliance on Qualified Electronic Signature.

QCP-w-PSD2 Certificates include additional information in accordance with ETSI TS 119 495 describing the PSP roles, Authorisation Number, and NCA.

2.4.5. Closed Community Certificates

Closed Community Issuing CAs can, under contract, create Certificate Profiles to match the QuoVadis Standard Commercial Certificate for issuance to employees and affiliates.

Certificates issued by Closed Community Issuing CAs are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone certificate policy to its community issue various certificates that differ from the Standard Commercial Certificate.

QuoVadis must approve all closed community certificate policies to ensure that they do not conflict with the terms of the QuoVadis CP/CPS. Refer to the QuoVadis CP/CPS for further details of closed community certificates. Under no circumstances can Closed Community Issuing CAs issue Qualified Certificates under European Digital Signature law.

2.4.6. QuoVadis Device Certificates

Purpose
QuoVadis Device Certificates are intended for a variety of uses including for Time-stamp Authority (TSA) applications (1.3.6.1.4.1.8024.1.600). QuoVadis Device Certificates that have the serverAuth Extended Key Usage comply with the CA/B Forum Baseline Requirements.
Registration Process
QuoVadis acts as Registration Authority (RA) for Device Certificates it issues. Before issuing a Device Certificate, QuoVadis performs procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and/or Organisation name to be included in the Certificate, and has accepted a Subscriber Agreement for the requested Certificate. Documentation requirements for organisation Applicants may include, Certificate of Incorporation, Memorandum of Association, Articles of Incorporation or equivalent documents. Documentation requirements for individual Applicants may include trustworthy, valid photo ID issued by a Government Agency (such as a passport). QuoVadis may accept at its discretion other official documentation supporting an application. QuoVadis may also use the services of a third party to confirm Applicant information.

2.4.7. TLS/SSL Certificates

i) **Business SSL Certificates** are Certificates for which limited authentication and authorisation checks are performed on the Subscriber and the individuals acting for the Subscriber (OID 1.3.6.1.4.1.8024.0.2.100.1.1).
ii) **Extended Validation SSL Certificates** are issued in compliance with the "Guidelines for the Issuance and Management of Extended Validation Certificates" published by the CA/Browser Forum (OID 1.3.6.1.4.1.8024.0.2.100.1.2).
iii) **Qualified Website Authentication Certificates** (QWAC) are Certificates issued in compliance with the eIDAS Regulation (OID 0.4.0.194112.1.4) or for PSD2 (also with OID 0.4.0.19495.3.1). *See* also Section 2.6.6.

Validation of Domain and Email Authorisation and Control
For each FQDN listed in a TLS Certificate, QuoVadis confirms that the Applicant either is the Domain Name Registrant or has control over the FQDN by methods described in Section 3.2.2.4 of the CA/Browser Forum Baseline Requirements.

QuoVadis verifies an Applicant's or Organisation's right to use or control of an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following:

- By verifying domain control over the email Domain Name using one of the procedures listed in this section; or
- by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response within a limited period of time that includes the Random Value to indicate that the Applicant controls that same email address.

Authentication For An IP Address
For each IP Address listed in a Certificate, QuoVadis confirms that the Applicant controlled the IP Address by methods described in Section 3.2.2.5 of the CA/Browser Forum Baseline Requirements.

2.4.8. Code Signing Certificates

Code Signing Certificates are Certificates issued in compliance with the Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates ("Code Signing Baseline Requirements"). (OID 1.3.6.1.4.1.8024.0.2.200.1.1). This includes identification of the Subscriber by a verified organization name and certificate revocation for any misrepresentation or publication of malicious code.

3. RELIANCE LIMITS

See Section 9.8 of the relevant QuoVadis CP/CPS, which does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CP/CPS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) QUOVADIS AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "QUOVADIS ENTITIES") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF; AND (B) THE QUOVADIS ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO QUOVADIS IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF

WHETHER QUOVADIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CP/CPS, MAY BE MADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER.

- For Swiss Qualified Certificates, QuoVadis liability is in accordance with Articles 17, 18, 19 of ZertES.
- For EU Qualified Certificates, QuoVadis liability is in accordance with Extract 37 and Article 13 of the eIDAS Regulation.

4. OBLIGATIONS OF SUBSCRIBERS

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorised. Subscribers are required to notify QuoVadis and any applicable RA if a change occurs that could affect the status of the Certificate.
QuoVadis requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of QuoVadis and all Relying Parties and Application Software Vendors. This make take the form of either:

i) The Applicant's agreement to the Subscriber Agreement with QuoVadis; or

ii) The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to QuoVadis, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

i) Securely generate its Private Keys and protect its Private Keys from compromise, and exercise sole and complete control and use of its Private Keys.;

ii) Provide accurate and complete information when communicating with QuoVadis, and to respond to QuoVadis' instructions concerning Key Compromise or Certificate misuse;

iii) Confirm the accuracy of the certificate data prior to installing or using the Certificate;

iv) For Qualified Certificates (a) if the policy requires the use of a QSCD, Electronic Signatures must only be created by a QSCD, (b) in the case of natural persons, the Private Key should only be used for Electronic Signatures, and (c) in the case of legal persons, the Private Key must be maintained and used under the control of the Subscriber and it should only be used for Electronic Seals.

v) Promptly (a) request revocation of a Certificate, cease using it and its associated Private Key, and notify QuoVadis if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (b) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

vi) For Remote Identity Verification, use the identity proofing software distributed by QuoVadis. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;

vii) Ensure that individuals using Certificates on behalf of an organisation have received security training appropriate to the Certificate;

viii) Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, including only installing TLS/SSL Server Certificates on servers accessible at the Domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent; and

ix) Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that QuoVadis notifies the Subscriber that the QuoVadis PKI has been compromised.

Subscriber Agreements may include additional representations and warranties.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. A Relying Party must exercise Reasonable Reliance as set out in this Section.

i) Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by QuoVadis related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available).

   - to be relied upon as an EU Qualified Certificate, the CA/trust anchor for the validation of the Certificate shall be as identified in a service digital identifier of an EU Trusted List entry with service type identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC" for a QTSP.
   - ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted Lists. ETSI TS 119 172-4 describes how to validate a digital signature to determine whether it can be considered as an EU Qualified electronic signature or seal.

ii) Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by QuoVadis.

iii) Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties reliance will be deemed reasonable if:

   - the attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
   - the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
   - the Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
   - the Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
   - the Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Certificate being relied upon;
   - the Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
   - the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
   - the identity of the Subscriber is displayed correctly by utilising trusted application software; and
   - any alterations arising from security changes are identified by utilising trusted application software.

If the circumstances indicate a need for additional assurances, it is Relying Parties' responsibility to obtain such assurances. A Relying Party shall make no assumptions about information that does not appear in a Certificate. All obligations within this Section relate to Reasonable Reliance on the validity of a Digital

Signature, not the accuracy of the underlying electronic record. Relying Party Agreements may include additional representations and warranties.

6. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

OTHER THAN AS PROVIDED IN SECTION 9.6.1 OF THE CP/CPS, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, QUOVADIS DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. QUOVADIS DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

QuoVadis does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time. Subscriber's sole remedy for a defect in the Certificates is for QuoVadis to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that QuoVadis has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Certificates or combination of the Certificates with other products and services by parties other than QuoVadis, or (ii) Subscriber's breach of any provision of the Subscriber Agreement

7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT CERTIFICATE POLICY

The QuoVadis Master Services Agreement references and makes the Certificate Terms of Use, Privacy Policy and relevant QuoVadis CP/CPS part of the Terms and Conditions. The itsme Issuing CA provides its own Terms and Conditions. The relevant documents are available online at https://www.quovadisglobal.com/repository.

8. PRIVACY POLICY

QuoVadis follows the Privacy Notices posted on its website when handling personal information. *See* https://www.quovadisglobal.com/privacy-policy which also includes privacy information for Remote Identity Verification. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9. REFUND POLICY

QuoVadis or Issuing CAs under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements. *See* Section 9.1.5 of the CP/CPS

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. GOVERNING LAW

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have

exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-section (i) above, will each depend on where Customer is domiciled, as set forth in the table below.

In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Customer is Domiciled in:	**Governing Law is:**	**Court or arbitration body with exclusive jurisdiction:**
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah
Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in the below city corresponding to the QuoVadis contracting entity listed in the Order Form. For QV CH: Zurich For QV NL: Amsterdam For QV DE: Munich For QV BE/DigiCert Europe: Brussels For QV UK: London
Japan	Japan	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne
A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

10.2. DISPUTE RESOLUTION

See section 9.13 of the applicable QuoVadis CP/CPS. To the extent permitted by law, before a Participant in the QuoVadis PKI files suit or initiates an arbitration claim with respect to a dispute, Participant shall notify QuoVadis, and any other party to the dispute for the purpose of seeking business resolution. Both Participant and QuoVadis shall make good faith efforts to resolve such dispute via business discussions. If the dispute is

not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this CP/CPS and other relevant agreements.

- Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.
- Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

  - For Swiss Qualified Certificates such arbitration shall, unless agreed otherwise between the parties, take place in Switzerland.
  - For Qualified Certificates issued in accordance with eIDAS, arbitration for disputes related to financial or commercial matters will be dealt with in the country of the relevant QuoVadis entity named in the contract with the client. Arbitration for Certificate-related disputes will be dealt with in the country named in relevant QuoVadis Issuing CA Certificate.

11. CA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

Refer to https://www.quovadisglobal.com/accreditations for a list of QuoVadis' audits and accreditations.