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:	August 25, 2020
Version:	1.9

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 Digital Certificates issued by QuoVadis are issued. This PDS relates to the following CP/CPS documents:

- CP/CPS for QuoVadis Root Certification Authority, 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 G1. 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; addition of complaints procedure.

TABLE OF CONTENTS

1. CA CONTACT INFO

Bermuda and Group

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11,
Bermuda

Mailing Address:
QuoVadis Limited
Suite 1640
48 Par-La-Ville Road
Hamilton HM-11
Bermuda

Phone: +1-441-278-2800
Website: www.quovadisglobal.com
Compliance email: compliance@quovadisglobal.com
Problem reporting: https://www.quovadisglobal.com/certificate-revocation
Customer complaints: qvcomplaints@digicert.com

Netherlands QuoVadis Trustlink BV Nevelgaarde 56 noord 3436 ZZ Nieuwegein The Netherlands Phone: +31 (0) 30 232-4320	**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	**Switzerland** QuoVadis Trustlink Schweiz AG Poststrasse 17, Postfach 9001 St. Gallen, Switzerland Phone: +41-71-272-60-60
United Kingdom QuoVadis Online Limited 2 Harbour Exchange Square London, E14 9GE United Kingdom Phone: +44 (0) 333-666-2000	

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. The procedures for Digital Subscriber registration and validation are described below for each type of Digital 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"). 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 the "QV Advanced" Certificate Class 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
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

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	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
	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

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 **Extended Key Usage** smartcardlogon clientAuth emailProtection documentSigning	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	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)
Encryption	**Key Usage** keyEncipherment **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	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Not Allowed

2.3. QV STANDARD

Purpose
Standard Digital 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 Digital 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 Subscriber.

2.4. QV ADVANCED

Purpose
QV Advanced Digital Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, 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. Unless the Subscriber has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Subscriber shall include the following: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. If the subject is a natural person evidence shall be provided of: • Full name (including surname and given names consistent with applicable law and national identification practices); and • Date and place of birth, reference to a 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 who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. 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.

2.5. 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. 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+ certificate class. These certificates are issued out of the "QuoVadis Swiss Regulated CAs" and have the notice text "regulated certificate" in the CertificatePolicies user notice. Swiss Regulated Certificates can be issued to natural and legal persons.

Registration Process

QuoVadis Advanced+ Digital 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 described in 2.3 above.

QuoVadis Advanced+ Digital 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.

2.5.1. 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.

Evidence of the Subscriber's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence according to ZertES. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES. Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 Subscriber is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorisation from an authorised Organisation representative; and
- Evidence that the Subscriber is associated with the organisational entity.

Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS PUB 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 issued by QuoVadis have a maximum validity of three years.

2.5.2. 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.

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 compliant Qualified Certificate. The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence by an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person according to ZertES

Evidence shall be provided of:

- Full name of the organisational entity (private organisation, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices); and
- When applicable, the association between the legal person and the 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.

For the authorised representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

Evidence of the Certificate applicant identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence according to

ZertES. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS PUB 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 issued by QuoVadis have a maximum validity of three years.

2.6. QV QUALIFIED

2.6.1. 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.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence of the natural person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the eIDAS Regulation [i.1].

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

Evidence may be provided on behalf of the subject by the RA. However, the subject remains responsible for the content of the Certificate.

If the Subscriber is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Subscriber is associated with the organisational entity.

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.

2.6.2. 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 Digital 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 described in 2.5.1 above. The only difference is that these QCP-n certificates do not use a QSCD for the protection of the private key.

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.

2.6.3. 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 Digital 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).

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence by an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name of the organisational entity (private organisation, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices); and
- When applicable, the association between the legal person and the 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.

For the authorised representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

These Digital 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.

2.6.4. 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 Digital 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 described in 2.6.3 above. The only difference is that these QCP-l certificates do not use a QSCD for the protection of the private key.

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.

2.6.5. Swiss Qualified Certificate

Purpose

QV Qualified Switzerland 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 CertificatePolicies user notice. QV Qualified Switzerland Certificates are used to sign documents electronically. The digital signature is tamperproof and legally equivalent to a handwritten signature.

Registration Process

QV Qualified Switzerland Certificates are issued in accordance with the ZertES requirements using thea QuoVadis Signing Service or HSM or PrimoSign. The guidelines in TAV-ZERTES apply to the specification of QV Qualified Switzerland Certificates.

Evidence of the Subscriber's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES. Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 Subscriber is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorisation from an authorised Organisation representative; and
- Evidence that the Subscriber is associated with the organisational entity.

Private Keys for QV Qualified Switzerland Certificates are generated and stored on an HSM Hardware Security Module that meets the ZertES requirementsFIPS PUB 140-2, level 3 or EAL 4 standards. This 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 Qualified Switzerland Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour.

2.6.6. 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. The identity of the legal person and, if applicable, any specific attributes of the legal person, shall be verified:

- by the physical presence of an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which QuoVadis can prove the equivalence.

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

2.7. 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.

2.8. QUOVADIS DEVICE

Purpose
QuoVadis Device Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. QuoVadis Device Certificates (i.e. with the OID 1.3.6.1.4.1.8024.1.600 in Certificate Policies) that have the Server Authentication 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. **Validation of Domain and Email Authorisation and Control** For each FQDN listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by: i) Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation) ii) Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorisation Domain Name (ADN). Performed in accordance with BR section 3.2.2.4.4; iii) Confirming the Applicant's control over the requested ADN (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value in a DNS record. Performed in accordance with BR section 3.2.2.4.7; iv) Confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8; v) Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12; vi) Confirming the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact and then receiving a confirming response utilising the Random Value. The relevant CAA

Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance with BR Section 3.2.2.4.13;

vii) Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the ADN and then receiving a confirming response utilising the Random Value, performed in accordance with BR Section 3.2.2.4.14;

viii) Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call can confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with BR Section 3.2.2.4.15;

ix) Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call can confirm control of multiple ADN provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with BR Section 3.2.2.4.16;

x) Confirming the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response. Each phone call can confirm control of multiple domains provided that the same DNS CAA Phone Contact phone number is listed for each domain being verified and a confirming response is provided for each ADN. Performed in accordance with BR Section 3.2.2.4.17;

xi) Confirming the Applicant's control over the requested FQDN by confirming the presence of an agreed-upon Random Value under the "/.well-known/pki-validation" directory. Performed in accordance with BR section 3.2.2.4.18;

xii) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method, performed in accordance with BR Section 3.2.2.4.19. . This method is suitable for validating Wildcard Domain Names; or

xiii) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the ALPN Extension, performed in accordance with BR Section 3.2.2.4.20. This method is NOT suitable for validating Wildcard Domain Names.

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:

i) By verifying domain control over the email Domain Name using one of the procedures listed in this section; or

ii) 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.

QuoVadis maintains a list of High Risk Domains and has implemented technical controls to prevent the issuance of Certificates to certain domains. QuoVadis follows documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval.

Authentication For An IP Address

For each IP Address listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

i) Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;

ii) Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilising the Random Value, performed in accordance with BR Section 3.2.2.5.2;

iii) Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;

iv) Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address RA, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;

v) Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or

vi) Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

2.9. TLS/SSL AND CODE SIGNING CERTIFICATES

QuoVadis issues four forms of Certificates according to the terms of the QuoVadis Root CA2 CP/CPS (www.quovadisglobal.com/repository):

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 Certificates issued in compliance with the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) published by the CA/Browser Forum. The EV Guidelines are intended to provide enhanced assurance of identity of the Subscriber by enforcing uniform and detailed validation procedures across all EV-issuing CAs (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). QuoVadis is listed on the Trust List for the Netherlands (https://webgate.ec.europa.eu/tl-browser/#/trustmark/NL/NTRNL-30237459).
iv) Trusted Code Signing Certificates are Certificates issued in compliance with the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates ("Code Signing Minimum Requirements") published at https://aka.ms/csbr. (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

Digital Subscribers are required to act in accordance with the CP/CPS and the relevant Subscriber/Subscriber Agreement. A Digital Subscriber represents, warrants and covenants with and to QuoVadis, Relying Parties, Application Software Vendors and the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Subscriber, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. *See* Appendix A.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing CA, Registration Authority, or QuoVadis immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorised viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorised use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Subscriber's Public Key. In the case of legal persons, the private key must be maintained and used under the control of the Subscriber and is recommended to be used only for electronic seals.
- If the policy requires the use of a Qualified Electronic Signature Creation Device (QSCD), digital signatures must only be created by a QSCD.
- For Qualified certificates issued to natural persons, it is recommended that the Subscriber's key pair is only used for electronic signatures.
- Immediately notify the Issuing CA, Registration Authority or QuoVadis in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever. Following compromise, the use of the Subscriber's Private Key should be immediately and permanently discontinued. For certificates issued from the itsme sign Issuing CA G1 all revocation requests must be directed to the itsme first-line helpdesk.
- Take all reasonable measures to avoid the compromise of the security or integrity of the QuoVadis PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Subscriber.
- Discontinue the use of the digital signature Key Pair in the event that QuoVadis notifies the Subscriber that the QuoVadis PKI has been compromised.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Subscriber, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to be an Relying Party, a Party seeking to rely on a Digital Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement (https://www.quovadisglobal.com/repository) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by the CP/CPS.
- That the Certificate is being used in accordance with its Key-Usage field extensions.
- That the Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List (http://crl.quovadisglobal.com/<caname>.crl) or is made available via Online Certificate Status Protocol checking (http://ocsp.quovadisglobal.com) where 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.

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 following documents are available online at https://www.quovadisglobal.com/repository:

- Certificate Policy/Certification Practice Statements
- Subscriber Agreement, Certificate Terms of Use, Master Services Agreement
- Relying Party Agreement
- Code Signing Certificate Subscriber Agreement

- QuoVadis Time-Stamp Disclosure Statement
- QuoVadis Time-Stamp Policy/Practice Statement
- QuoVadis Time-Stamp Subscriber Agreement

In the context of the itsme Issuing CA the Subscriber Agreement is referred to as the Terms and Conditions for itsme.

8. PRIVACY POLICY

QuoVadis follows the Privacy Notices posted on its website when handling personal information. *See* https://www.quovadisglobal.com/privacy-policy. 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 (https://www.quovadisglobal.com/repository).

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. CUSTOMER COMPLAINTS

QuoVadis is committed to ensuring that we provide the best services and products possible to our customers. However, we do realise sometimes customers may want to pass on their concerns. In the event you have feedback, please contact us at qvcomplaints@digicert.com. We will acknowledge of the receipt of your feedback within 24 hours and will provide a more specific response from the relevant department within 5 working days. In the majority of cases the relevant team leader will be able to respond to your feedback and resolve any outstanding issues without the need for escalation. In some cases, it may be necessary to involve other departments and team members to ensure the correct response is provided to you. This is at the discretion of the team leader or manager handling the process. You will be informed if this is necessary.

10.2. 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 laws of:	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/DC BE: Brussels For QV UK and QVA: 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

10.3. 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.