PKI Disclosure Statement PKIoverheid

Effective Date: 29 April 2020
Version: 1.4

QuoVadis TrustLink B.V.
Nevelgaarde 56
3436 ZZ Nieuwegein
Tel: +31 302324320
Fax: +31 302324329

Important Notice about this Document

This document is the PKI Disclosure Statement for PKIoverheid herein after referred to as the PDS. This document does not substitute or replace the Certification Practice Statement (CPS) under which digital certificates issued by QuoVadis Limited (QuoVadis, a company of DigiCert, Inc.) are issued. This PKI Disclosure Statement relates to the QuoVadis PKIoverheid CPS document.

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

The purpose of this document is to summarise the key points of the QuoVadis PKIoverheid CPS for the benefit of Subscribers, Certificate Holders and Relying Parties.

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 August 2018	1.0	First version
QuoVadis PMA	11 July 2019	1.1	Updates for dispute resolution and more references to Private CPS and certificate classes
QuoVadis PMA	10 September 2019	1.2	Updates to reflect consolidated PKIoverheid CP/CPS and where QuoVadis manages private keys on behalf of the Certificate Holder (remote QSCD)
QuoVadis PMA	20 March 2020	1.3	Review and alignment with PKIoverheid CPS
QuoVadis PMA	29 April 2020	1.4	General review, addition of URL for privacy policy and correction of descriptions in 2.1.

CONTENTS

1. TRUST SERVICE PROVIDER (TSP) CONTACT INFO 1
2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE 1
   - 2.1. QuoVadis Certificate Classes 1
   - 2.2. PKIo advanced 3
   - 2.3. PKIo Qualified 4
     - 2.3.1. PKIo Qualified Certificate issued to a natural person on a QSCD 4
     - 2.3.2. PKIo Qualified Certificate issued to a legal person on a QSCD 5
   - 2.4. QuoVadis Qualified Website Authentication (QCP-w) 6
   - 2.5. Services Server Certificates 2
3. RELIANCE LIMITS 2
4. OBLIGATIONS OF SUBSCRIBERS 3
5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES 3
6. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY 4
7. APPLICABLE AGREEMENTS, CP/CPS 4
8. PRIVACY POLICY 4
9. REFUND POLICY 4
10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION 4
    - 10.1. Governing Law 4
    - 10.2. Dispute Resolution 5
11. TSP AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT 5

1. TRUST SERVICE PROVIDER (TSP) CONTACT INFO

1.1. QUOVADIS TRUSTLINK BV

Address:	Nevelgaarde 56 noord 3436 ZZ Nieuwegein The Netherlands
Telephone:	Phone: +31 (0) 30 232-4320 Phone: +1-441-278-2800
Website:	www.quovadisglobal.com
Email:	info.nl@quovadisglobal.com

1.2. REVOCATION

The online revocation facility via the QuoVadis website TrustLink Enterprise is available 24 hours a day, 7 days a week via https://tl.quovadisglobal.com. The QuoVadis support line +31 (0) 30 232 4320 is also available outside CET time zone office hours via +1 651 229 3456.

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI a PKIoverheid Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. The procedures for Digital Certificate Holder 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").

2.1. QUOVADIS CERTIFICATE CLASSES

PKIo Certificate type	**Description**	**Key usages**	**Certificate Policy OID**	**Requires token?**
Personal User Authentication	Advanced certificate used for client authentication issued to a natural person linked to an organisation	Digital signature(client Authentication document Signing emailProtection)	2.16.528.1.1003.1.2.5.1	Yes
Personal User Encryption	Advanced certificate used for encryption issued to a natural person linked to an organisation	keyEncipherment dataEncypherment (document signing emailprotection)	2.16.528.1.1003.1.2.5.2	Yes
Personal User Non-Repudiation	Qualified certificate used for signing issued to a natural person linked to an organisation	Non-repudiation (Encrypting File System emailProtection)	2.16.528.1.1003.1.2.5.3	Yes

PKIo Certificate type	Description	Key usages	Certificate Policy OID	Requires token?
Organisation Service Authentication	Advanced certificate used for client authentication issued to an organisation	Digital signature (client Authentication document Signing emailProtection)	2.16.528.1.1003.1.2.5.4	Yes
Organisation Service Encryption	Advanced certificate used for encryption issued to an organisation	keyEncipherment dataEncypherment (Encrypting File System emailprotection)	2.16.528.1.1003.1.2.5.5	Yes
Organisation Service Seal	qualified certificate used for signing issued to an organisation	Non-repudiation (document Signing emailProtection)	2.16.528.1.1003.1.2.5.7	Yes
Personal Citizen Authentication	Advanced certificate used for client authentication issued to a natural person	Digital signature(client Authentication document Signing emailProtection)	2.16.528.1.1003.1.2.3.1	Yes
Personal Citizen Non-Repudiation	Advanced certificate used for encryption issued to a natural person	keyEncipherment dataEncypherment (document signing emailprotection)	2.16.528.1.1003.1.2.3.2	Yes
Personal Citizen Encryption	Qualified certificate used for signing issued to a natural person	Non-repudiation (Encrypting File System emailProtection)	2.16.528.1.1003.1.2.3.3	Yes
Organisation Service Server	Organisation validated TLS/SSL certificate	Digital signature key encipherment (server auth client auth)	2.16.528.1.1003.1.2.5.6	no
EV policy (QWAC)	Extended validation TLS/SSL certificate may contain QC statements and become qualified website authentication certificate	Digital signature key encipherment (server auth client auth)	2.16.528.1.1003.1.2.7	No
Private Personal Authentication	Certificate used for client authentication issued to a natural person linked to an organisation from a non public trusted root	Digital signature(client Authentication document Signing emailProtection)	2.16.528.1.1003.1.2.8.1	Yes
Private Personal Non-Repudiation	Qualified certificate used for signing issued to a natural person linked to an organisation from a non public trusted root	Non-repudiation (document Signing emailProtection)	2.16.528.1.1003.1.2.8.2	Yes

PKIo Certificate type	Description	Key usages	Certificate Policy OID	Requires token?
Private Personal Encryption	Certificate used for encryption issued to an organisation from a non public trusted root		2.16.528.1.1003.1.2.8.3	Yes
Private Services authenticiteit	Advanced certificate used for client authentication issued to an organisation	Digital signature(client Authentication document Signing emailProtection)	2.16.528.1.1003.1.2.8.4	Yes
Private Services vertrouwelijkheid	Advanced certificate used for encryption issued to an organisation	keyEncipherment dataEncypherment (document signing emailprotection)	2.16.528.1.1003.1.2.8.5	Yes
Private Services Server	Organisation validated TLS/SSL certificate from a non public trusted root	Digital signature key encipherment (server auth client auth)	2.16.528.1.1003.1.2.8.6	No

2.2. PKIO ADVANCED

PKIo 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. Their specific use is determined by the certificate type (key usages) and the subject of the certificate.

The content of these certificates meet the relevant requirements from:

- ETSI EN 319 411-1: Certificate Profiles; Part 1: Overview and common data structures
- PKIoverheid PVE part 3A/3B/3C/3I
- PKIoverheid PVE basiseisen
- PKIoverheid PVE aanvullende eisen

Registration Process

Validation procedures for QuoVadis Advanced Digital Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1.

Unless the Certificate Holder 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 Certificate Holder 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 Certificate Holder 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 Certificate Holder is affiliated with the legal person.

If the Certificate Holder 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 Certificate Holder 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.

2.3. PKIO QUALIFIED

2.3.1. PKIo Qualified Certificate issued to a natural person on a QSCD

The purpose of an PKIoverheid Qualified certificates is to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation").

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key. In some cases, QuoVadis generates and manages private keys on behalf of the Certificate Holder and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 0.4.0.19431.1.1.3 OID in certificate policies. This OID is the EUSCP: EU SSASC Policy 'eu-remote-qscd' OID defined in ETSI TS 119 431-1.

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).

The content of these certificates meets 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
- PKIoverheid PVE part 3A/3C/3I
- PKIoverheid PVE basiseisen
- PKIoverheid PVE aanvullende eisen

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 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:

i. by the physical presence of the natural person; or

ii. 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 Regulation (EU) N° 910/2014 [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.

If the Certificate Holder 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 Certificate Holder is associated with the organisational entity.

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.

2.3.2. PKIo Qualified Certificate issued to a legal person on a QSCD

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

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person certificates an updated version of this CP/CPS will be published.

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key. In some cases, QuoVadis generates and manages private keys on behalf of the Certificate Holder and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 0.4.0.19431.1.1.3 OID in certificate policies. This OID is the EUSCP: EU SSASC Policy 'eu-remote-qscd' OID defined in ETSI TS 119 431-1.

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
- PKIoverheid PVE part 3B
- PKIoverheid PVE basiseisen
- PKIoverheid PVE aanvullende eisen

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:

i. by the physical presence by an authorized representative of the legal person; or

ii. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized 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 authorized 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.

2.4. QUOVADIS QUALIFIED WEBSITE AUTHENTICATION (QCP-W)

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 certificate 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:

- The EV Guidelines;
- ETSI EN 319 411-2;
- ETSI EN 319 412-4; and
- ETSI EN 319 412-5:
- PKIoverheid PVE part 3F
- PKIoverheid PVE basiseisen
- PKIoverheid PVE aanvullende Eisen

Registration Process

The verification requirements for a QuoVadis Qualified Website Authentication (QCP-w) certificate are consistent with the vetting requirements for a PKIoverheid EV TLS/SSL certificate (described in the PKIoverheid 3F 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:

i. by the physical presence of an authorized representative of the legal person; or

ii. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which QuoVadis can prove the equivalence.

2.5. SERVICES SERVER CERTIFICATES

QuoVadis issues three forms of Certificates according to the terms of the QuoVadis PKIoverheid 3E/3F CPS (www.quovadisglobal.com/repository):

i. PKIoverheid services server Certificates are Certificates for which limited authentication and authorization checks are performed on the Subscriber and the individuals acting for the Subscriber.

ii. PKIoverheid Extended Validation Certificates are TLS/SSL 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.

iii. Qualified Website Authentication Certificates (QWAC) are TLS/SSL 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 additionally these certificates meet relevant requirements from ETSI EN 319 411-2 and 319 412-4

3. RELIANCE LIMITS

Refer to section 9.8 of the relevant PKIoverheid CP/CPS (www.quovadisglobal.com/repository) for reliance limits. QuoVadis' liability for breach of its obligations pursuant to the QuoVadis CP/CPS shall, in the absence of fraud or willful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below:

Loss Limits/ Reliance Limits	**Maximum per Certificate**
Certificates	US$250,000

In no event shall QuoVadis' liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular Digital Certificate to the intent that the loss limits reflect QuoVadis' total potential cumulative liability per Digital Certificate per year (irrespective of the number of claims per Digital Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Digital Certificate in any one year of that Digital Certificate's life cycle.

All events involved in the generation of the CA key pairs are recorded. This includes all configuration data and registration information used in the process. Audit logs are retained as archive records for a period no less than seven years for Key and Digital Certificate information.

4. OBLIGATIONS OF SUBSCRIBERS

Subscribers agree to the following obligations in applying for, using and managing a Certificate issued by QuoVadis under PKIoverheid;

a. The obligation to provide the TSP with accurate and complete information in accordance with the requirements of the present document, particularly with regards to registration;
b. The obligation for the key pair to be only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person;
c. The prohibition of unauthorized use of the subject's private key;
d. If the Subscriber has generated their own keys, then;
    a. The recommendation to generate the subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP;
    b. The recommendation to use the key length and algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the certificate;
e. If the Subscriber or Subject generates the subject's keys and certificate key usage is for Non-repudiation (signing), Digital Signatures or Key Encipherment, then;
    a. When the Subject is a natural person there is an obligation for the subject's private key to be maintained under the Subject's sole control;
    b. When the Subject is a legal person there is an obligation for the subject's private key to be maintained under the Subject's sole control;
f. The obligation to only use the Subject's private keys for cryptographic functions within the secure cryptographic device;
g. The obligation to notify the TSP, without delay, if any of the following occur up to the end of the Certificate validity period;
    a. If the Subject's private key has been lost, stolen, potentially compromised;
    b. Where control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    c. Where there are inaccuracies or changes to the Certificate content, as notified to the Subscriber or Subject;
h. The obligation, following compromise of the Subject's private key, to immediately and permanently discontinue use of this key, except for key decipherment, and;
i. The obligation, in case of being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the Subject.

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

Authorised 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 Digital Certificate for any given purpose and that the use is not prohibited by the CP/CPS.
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.
- That the Digital 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.

5. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment (save as may arise directly from breach of the CPS), wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis' liability to any person for damages arising under, out of or related in any way to the CP/CPS, Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. QuoVadis shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the QuoVadis PKI (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the QuoVadis PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon the foregoing as a condition and inducement to permit that person to participate within the QuoVadis PKI.

Refer to the relevant PKIoverheid CPS (www.quovadisglobal.com/repository) for further detail as to liability and warranties.

6. APPLICABLE AGREEMENTS, CP/CPS

The CP/CPS documents and applicable agreements are available online at www.quovadisglobal.com/repository.

7. PRIVACY POLICY

Refer to the QuoVadis Privacy Notice at: https://www.quovadisglobal.com/privacy-policy/

8. 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. Refer to section 9.1.5 of the relevant CPS (www.quovadisglobal.com/repository).

9. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

9.1. GOVERNING LAW

Subscribers and Relying Parties shall use QuoVadis Certificates and any other related information and materials provided by QuoVadis only in compliance with all applicable laws and regulations. QuoVadis may refuse to issue or may revoke Certificates if, in the reasonable opinion of QuoVadis, issuance or the continued use of the QuoVadis Certificates would violate applicable laws or regulations.

QuoVadis Certificates issued by QuoVadis are governed by the laws of the country referred to in the Subscriber Agreement for the Certificate in question, without reference to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods.

9.2. DISPUTE RESOLUTION

Complaints can be communicated to QuoVadis via the QuoVadis website using the "Contact Us" link at https://www.quovadisglobal.com/ContactUs.aspx.

Complaints can also be communicated to QuoVadis verbally by phoning the relevant QuoVadis office. A list of QuoVadis offices and contact details are provided at https://www.quovadisglobal.com/Locations.aspx. Complaints will be considered by QuoVadis management and then the appropriate steps will be taken.

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a "participant" within the QuoVadis PKI) arising out of or relating to the QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

Dispute between the Root CA and an Issuing CA is dealt with under Dutch Law.

Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.

Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

For Qualified Certificates issued from Issuing CAs listed on the Netherlands national Trusted List, such arbitration shall, unless agreed otherwise between the parties take place in The Netherlands.

10. TSP AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

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