PKI Disclosure Statement **for PKIoverheid**

Effective Date: 25 August 2020
Version: 1.6

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

Important Notice about this Document

This document is the DigiCert + QuoVadis 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 are issued by QuoVadis Trustlink B.V. (a subsidiary of DigiCert Inc.).

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

The purpose of this document is to summarise the key points of the QuoVadis CPS for PKIoverheid for the benefit of Subscribers, Subjects, 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 CPS and where QuoVadis manages Private Keys on behalf of the Subscriber (remote QSCD)
QuoVadis PMA	28 March 2020	1.3	Review and alignment with PKIoverheid CPS
QuoVadis PMA	29 April 2020	1.4	Review and alignment with PKIoverheid CPS
QuoVadis PMA	6 August 2020	1.5	Review and alignment with PKIoverheid CPS
QuoVadis PMA	25 August 2020	1.6	Revisions including addition of PKIo Domain Server 2020 and removal of PKIo EV SSL.

CONTENTS

1. TRUST SERVICE PROVIDER (TSP) CONTACT INFO

Enquiries or other communication about this document should be addressed to the QuoVadis Policy Management Authority (PMA).

Address:	QuoVadis TrustLink B.V. Nevelgaarde 56 noord 3436 ZZ Nieuwegein, The Netherlands
Telephone:	Phone: +31 (0) 30 232-4320
Website:	https://www.quovadisglobal.nl
Email:	info.nl@quovadisglobal.com
Support (non revocation) requests	nl.support@quovadisglobal.com

1.1. CERTIFICATE PROBLEM REPORTS

To notify QuoVadis of a case suspected Private Key compromise, misuse, fraud, inappropriate conduct, or any other matter related to Certificates or this document, please contact compliance@quovadisglobal.com. For additional information on problem reporting see https://www.quovadisglobal.com/certificate-revocation.

1.2. REVOCATION REPORTING

Subscribers may revoke their own Certificates 24x7 via the QuoVadis Portal at https://tl.quovadisglobal.com/.

QuoVadis will revoke a Certificate following a valid request to do so from the Subscriber or other third parties (including organisations of Registered Professionals or PKIoverheid regulators such as Logius). If revocation is requested by someone other than the Subscriber or Affiliated Organisation, QuoVadis or an RA will investigate the alleged basis for the revocation request prior to taking action.

Entities submitting Certificate revocation requests must list their identity and explain the reason for requesting revocation. QuoVadis or an RA will authenticate and log each revocation request. Typically, the following is required for revocation:

- Common Name
- Certificate serial number
- E-mail address of the Subject

See PKIoverheid CPS Section 4.9.

During Central European Time office hours, revocation requests may be made using the QuoVadis RA and support line +31 (0) 30 232 4320 or info.nl@quovadisglobal.com.

Outside of office hours, critical revocation requests may be made to +1 651 2293456.

2. QUOVADIS CERTIFICATE CLASSES FOR PKIOVERHEID

All QuoVadis PKIoverheid Certificates have a policy object identifier (OID) which identifies their use. Qualified Certificates meet the requirements of ETSI EN 319 411-2 and Regulation (EU) No. 910/2014 (the eIDAS Regulation).

PKIo Certificate type	Description	Key Usage	Certificate Policy OID	Requires token?
Personal User Authentication	Certificate used for client authentication issued to a natural person linked to an organisation	Client Authentication Document Signing Email protection	2.16.528.1.1003.1.2.5.1	Yes
Personal User Non-Repudiation	Certificate used for Signing, issued to a natural person linked to an organisation.	Document Signing Email protection	2.16.528.1.1003.1.2.5.2	Yes
Personal User Encryption	Certificate used for encryption, issued to a natural person linked to an organisation	Encrypting File System Email protection	2.16.528.1.1003.1.2.5.3	Yes
Organisation Service Authentication	Certificate used for client authentication issued to an organisation	Client Authentication Document Signing Email protection	2.16.528.1.1003.1.2.5.4	Yes
Organisation Service Encryption	Certificate used for encryption issued to an organisation	Encrypting File System Email protection	2.16.528.1.1003.1.2.5.5	Yes
Organisation Service Seal	Qualified Certificate used for signing issued to an organisation	Document Signing Email Protection	2.16.528.1.1003.1.2.5.7	Yes
Personal Citizen Authentication	Certificate used for client authentication issued to a natural person	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.3.1	Yes
Personal Citizen Non-Repudiation	Qualified Certificate used for signing issued to a natural person	Document Signing Email Protection	2.16.528.1.1003.1.2.3.2	Yes
Personal Citizen Encryption	Certificate used for encryption issued to a natural person	Encrypting File System Email Protection	2.16.528.1.1003.1.2.3.3	Yes
Organisation Service Server	Organisation Validation (OV) TLS/SSL Vertificate	Digital Signature Key Encipherment	2.16.528.1.1003.1.2.5.6	No
EV policy (QWAC) – Note: PKIo EV type Certificates will be revoked by August 31, 2020	Extended Validation (EV) TLS/SSL Certificate may contain QC statements and become Qualified Website Authentication Certificate	Digital Signature Key Encipherment	2.16.528.1.1003.1.2.7	No

PKIo Certificate type	Description	Key Usage	Certificate Policy OID	Requires token?
Private Personal Authentication	Certificate used for client authentication issued to a natural person linked to an organisation from a non public trusted root	Client Authentication Document Signing Email Protection	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	Document Signing Email Protection	2.16.528.1.1003.1.2.8.2	Yes
Private Personal Encryption	Certificate used for encryption issued to an organisation from a non public trusted root	Key Encipherment Data Encipherment	2.16.528.1.1003.1.2.8.3	Yes
Private Services Authentication	Certificate used for client authentication issued to an organisation	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.8.4	Yes
Private Services Encryption	Certificate used for encryption issued to an organisation	Key Encipherment Data Encipherment	2.16.528.1.1003.1.2.8.5	Yes
Private Services Server	Organisation Validation (OV) TLS/SSL Certificate from a non public trusted root	Client Authentication Server Authentication	2.16.528.1.1003.1.2.8.6	No
Domain CA 2020	Organisation Validation (OV) TLS/SSL Vertificate	Client Authentication Server Authentication	2.16.528.1.1003.1.2.5.9	No

See PKIoverheid CPS Appendix A.

2.1. PKIO ADVANCED CERTIFICATES

PKIo Advanced 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 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 Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1.

Unless the Applicant 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 an Applicant shall include the following.

If the Subject is a natural person (i.e., physical person as opposed to legal entity) evidence of the Subject's identity (e.g., name) shall be checked against this natural person either directly by physical presence of the person, 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 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 recognised 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; and
- a nationally recognised identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

2.2. PKIO QUALIFIED

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

The purpose of PKIoverheid Qualified Certificates is 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 Certificate use a Qualified Signature Creation Device (QSCD) meeting the requirements of Annex II of the eIDAS Regulation for the protection of the Private Key . In some cases, QuoVadis generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with eIDAS. 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 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 Certificates meet the 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.

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;
- Relevant existing registration information of the organisational entity; and
- Evidence that the Subscriber is associated with the organisational entity.

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

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 requirements defined by the eIDAS Regulation.

These Certificates use a Qualified Signature Creation Device (QSCD) meeting the requirements of Annex II of the eIDAS Regulation for the protection of the Private Key . In some cases, QuoVadis generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with eIDAS. 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 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 Certificates meet the 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 eIDAS Regulation.

Evidence shall be provided of:

- Full name of the organisational 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.

2.2.3. PKIo Qualified Website Authentication (QCP-w)

Note: It is no longer permitted to issue these types of Certificates. All remaining PKIo Qualified Website Authentication Certificates will be revoked by August 31, 2020. From September 1 onwards this information will no longer apply.

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

QCP-w Certificates are issued under the requirements of ETSI EN 319 411-2 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. 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; and
- ETSI EN 319 412-5:
- PKIoverheid PVE part 3F
- PKIoverheid PVE basiseisen
- PKIoverheid PVE aanvullende Eisen

Registration Process

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

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.

2.3. PKIO SERVICES SERVER CERTIFICATES

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

i. PKIoverheid Services Server Certificates for which limited authentication and authorisation checks are performed on the Subscriber and the individuals acting for the Subscriber.

ii. PKIoverheid Domain CA 2020 Certificates for which limited authentication and authorization checks are performed on the Subscriber and the individuals acting for the Subscriber.

3. RELIANCE LIMITS

Certificates issued may only be used for the purposes that they were issued, as explained in the PKIoverheid CPS, Subscriber Agreement, and Terms of Use as well as identified in the Key Usage field of the Certificate itself. Certificates are prohibited from being used for any other purpose that described, and all Certificate usage must be within the limits of applicable laws.

4. OBLIGATIONS OF SUBSCRIBERS

Subscribers are required to act in accordance with this CPS, Subscriber Agreement, and Terms of Use. Subscriber obligations include:

i) The obligation to provide QuoVadis with accurate and complete information in accordance with the requirements of the CPS, particularly with regards to registration;

ii) 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;

iii) The prohibition of unauthorized use of the Subject's Private Key;

iv) If the Subscriber has generated their own keys, then;

- The obligation 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 Certificate Policy of the PKIo PA;
- The obligation 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 Certificate Policy of the PKIo PA during the validity time of the certificate;

v) 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;

- The obligation for the Subject's Private Key to be maintained under the Subject's sole control;
- The obligation to only use the Subject's Private Keys for cryptographic functions within the secure cryptographic device;

vi) The obligation to notify QuoVadis, without delay, if any of the following occur up to the end of the Certificate validity period;

- If the Subject's Private Key has been lost, stolen, potentially compromised;
- Where control over the Subject's Private Key has been lost due to compromise of activation data (e.g., PIN code) or other reasons;

- Where there are inaccuracies or changes to the Certificate content, as notified to the Subscriber or Subject;

vii) The obligation, following compromise of the Subject's Private Key, to immediately and permanently discontinue use of this key, except for Key Decipherment; and

viii) 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.

See PKIoverheid CPS Section 1.3.3.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Relying Parties are entities that act in Reasonable Reliance on a Certificate issued by QuoVadis or a related Digital Signature.

i) that the Certificate intended to be relied upon is valid and has not been revoked, the Relying Party being obliged to check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate;

ii) 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;

iii) that the attributes of the Certificate relied upon are appropriate in all respects to the reliance placed upon that Certificate by the Relying Party including, without limitation to the generality of the foregoing, the level of Identification and Authentication required in connection with the issue of the Certificate relied upon;

iv) that the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted under this CPS;

v) that the Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;

vi) that the Relying Party has, at the time of that reliance, verified the Digital Signature, if any and confirmed it was created during the Operational Term of the Certificate being relied upon;

vii) that the Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software;

viii) that the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;

ix) that the identity of the Subscriber is displayed correctly by utilising trusted application software; and

x) that any alterations arising from security changes are identified by utilising trusted application software.

See PKIoverheid CPS Section 1.3.4.

6. LIMITATIONS OF LIABILITY

QuoVadis shall 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 CPS and related services.

See PKIoverheid CPS Section 9.8 for more information and liability limits. QuoVadis reserves the right, without liability, to reject any application for a Certificate.

7. APPLICABLE AGREEMENTS, CPS

The PKIoverheid CPS, Terms of Use, and Subscriber Agreement are available at https://www.quovadisglobal.com/repository

8. PRIVACY POLICY

The QuoVadis Privacy Notice is available at https://www.quovadisglobal.com/privacy-policy/. *See* PKIoverheid CPS Section 9.4.

9. REFUND POLICY

Details of refund policy may be contained in relevant contractual agreements. *See* PKIoverheid CPS Section 9.1.5.

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. GOVERNING LAW

All agreements entered into by QuoVadis under the PKIoverheid CPS are governed by Dutch law, unless otherwise specified. *See* PKIoverheid CPS Section 9.14.

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. *See* PKIoverheid CPS Section 9.15.

10.2. DISPUTE RESOLUTION

To the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, 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 CPS and other relevant agreements. *See* PKIoverheid CPS section 9.13.

11. TSP AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

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