PKI Disclosure Statement
for PKIoverheid

Effective Date:	September 30, 2020
Version:	1.7

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

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 Customer Complaints	nl.support@quovadisglobal.com

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	Extended Key Usage	Certificate Policy OID	Requires token?
Personal User Authentication	Certificate used for client authentication issued to a natural person linked to an organisation			

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.

- 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 ((e 3

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: ItTm[(N 7oTd[(a)-7 (e)e Tw 1. (tio)-12.2 (n)27 (og).3 (e)-7 (r)3.8 ( )-11.9 (7g).3 (e)-7 (r)3mi2 (t)-122 (t)-12.8 (e)-7 (3 (t

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 K

e h T obl[illegible]

    x 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 revo6.9 (S<Td8v)-3.1 (d (e)-6.9 (v)-3.17