# PKI Disclosure Statement for PKIoverheid

Effective Date: 6 August 2020
Version: 1.5

QuoVadis TrustLink B.V.3w 3.614w 3.613w 3.61Tw 1.024Z(T)1.7 Z1.3 (KI N (e)-7 () (dis5665.9 (T11.7 w)-1 ( e (e) ( g)1

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.<br>Nevelgaarde 56 noord<br>3436 ZZ Nieuwegein, The Netherlands |
| Telephone: | Phone: +31 (0) 30 232-4320 |
| Website: | https://www.quovadisglobal.nl |
| Email: | info.nl@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 CMS 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). *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. Typically, the following is required for revocation:

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

Outside of office hours, critical revocation requests may be made to +31 6 22934556. Normal (non revocation) support requests may be made to 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 | 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<br>Don | | |

| PKIo Certificate type | Description | Key Usage | Certificate Policy OID | Requires token? |
|---|---|---|---|---|

person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

If the Subjectis a natural person evidence shall be provided of:

- physical

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
- U

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 and 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)

## 8. PRIVACY POLICY

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