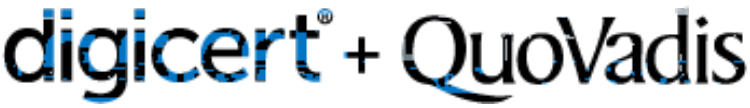
QuoVadis

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:	September 30, 2020
Version:	1.10

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 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

Version Control:

TABLE OF CONTENTS

1. CA CONTACT INFO

Website: https://www.quovadisglobal.com/
Repository: https://www.quovadisglobal.com/repository
Customer complaints email: qvcomplaints@digicert.com

Bermuda QuoVadis Limited Washington Mall 3F 7 Reid Street Hamilton HM-11 Bermuda Phone: +1-441-278-2800	**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	**Netherlands** QuoVadis Trustlink BV Nevelgaarde 56 noord 3436 ZZ Nieuwegein The Netherlands Phone: +31 (0) 30 232-4320
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

QuoVadis provides additional information for entities requiring assistance with revocation or an investigative report at https://www.quovadisglobal.com/certificate-revocation. Section 4.9.2 of the CP/CPS.

As of 15 Oct 2020, requests that Certificates be revoked due to keyCompromise must be submitted at https://problemreport.digicert.com/key-compromise providing the information outlined in Section 4.9 of the CP/CPS.

For other types of revocation requests, and for keyCompromise reporting before 15 Oct 2020, please email compliance@quovadisglobal.com.

Entities submitting Certificate revocation requests must explain the reason for requesting revocation. QuoVadis or an RA will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. QuoVadis will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorised representative of the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Affiliated Organisation, QuoVadis or an RA will investigate the alleged basis for the revocation request prior to taking action. Section 4.9.1 and 4.9.3 of the CP/CPS.

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Certificate Class	Description	Policy OID	Assurance Level	Requires token?

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	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

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				

Purpose
Standard 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 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.

Purpose
QV Advanced Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including Digital Signature, 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

according to ZertES. Only a valid passporintaliasnnassaccp8

- 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 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.

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

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 (0.4.0.006112.00612

Registration Process The verification requirements for a QuoVadis Qualified Website Authentication C

SUBSCRIBER TO QUOVADIS IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CO

Subscriber Agreements may include additional representations and warranties.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. A Relying Party must exercise Reasonable Reliance as set out in this Section.

i) Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by QuoVadis related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information 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.

ii) Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by QuoVadis.

iii) Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties reliance will be deemed reasonable if:

   - the attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
   - the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
   - 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;
   - the Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
   - the Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Certificate being relied upon;
   - the Relying Party ensures that the data signed has not bee.8 (ow)1.2 (d 12 (n)9.( )Te2 (n)9.-3.2 (rf6 (y)4 (h)3.8 (a
rified (d)f-32.94 (a)-6.(s)-6(0)0.8(p)-11(2n)(7a)-t)-3(2y-3(3-1EMC)-6.ti2(7)]Te)-(y)-9.1e-0.8.8-a)-(8)MCIDp

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

8. PRIVACY POLICY

QuoVadis follows the Privacy Notices posted on its website when handling personal information. https://www.quovadisglobal.com/privacy-policy. Personal information is only disclosed when the disclosure

Customer is Domiciled in:	Governing Law is :	Court or arbitration body with exclusive jurisdiction:
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 BE/DigiCert Europe: Brussels For QV UK: 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

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