QuoVadis

PKI Disclosure Statement

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 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 https://www.quovadisglobal.com/repository before you apply for or rely on a Certificate issued by QuoVadis.

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 2 Tw 20.181 0 (⊂

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement

TABLE OF CONTENTS

1. CA CONTACT INFO

Website: https://www.quovadisglobal.com/ hd(om/)]TJ 0s.lgva(l)12 i(om/)]TJewrcom/

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
QV Qualified	QuoVadis Qualified Certificate on a QSCD	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.400 ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCPn-qscd) 0.4.0.194112.1.3 (QCPl-qscd)	High	Yes Adobe AATL Approved
	QuoVadis Qualified Certificate on a QSCD where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.410	High	Yes
	Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCPn-qscd), with the OID 0.4.0.194112.1.2 EU Qualified Certificates issued to a legal person (QCP l-qscd), with the OID 0.4.0.194112.1.3	ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCPn-qscd) 0.4.0.194112.1.3 (QCPl-qscd)		Adobe AATL Approved
	QuoVadis Qualified Certificate not on a QSCD Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCPn), 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: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCPn) 0.4.0.194112.1.1 (QCPl)	High	No

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	QuoVadis Qualified Certificate not on a QSCD where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.60	High	No
	Relevant to the Policy in ETSI EN 319 411-2 for:	ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n)		
	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	0.4.0.194112.1.1 (QCP-l)		
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

QuoVadis provides test certificates for all types of Certificates.

2.2. KEY USAGE AND ARCHIVE

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 Class es			
		QV Standard	QV Advanced	QV Advanced +	QV Qualified
Signing and Encryption	Key Usage digitalSignature nonRepudiation keyEncipherment keyAgreement Extended Key Usage smartcardlogon clientAuth emailProtection documentSigning enrolmentAgent	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow not permitted)	Not Allowed
Signing	Key Usage digitalSignature nonRepudiation Extended Key Usage smartcardlogon clientAuth emailProtection documentSigning enrolmentAgent	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)
Encryption	Key Usage keyEncipherment keyAgreement Extended Key Usage emailProtection	Allowed (Escrow permitted)	Allowed (Escrow permitted)	Allowed (Escrow not permitted)	Not Allowed
Authentication	Key Usage digitalSignature Extended Key Usage smartcardlogon clientAuth enrolmentAgent	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Not Allowed

2.3. IDENTITY AUTHENTICATION

If the Subject is an Organisation (legal person), evidence shall be provided of:

i) Full name of the legal person;

ii) 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; and

iii) When applicable, the association between the legal person and any 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.

If the Subject is a natural person, evidence shall be provided to deliver unique identification of the Applicant, including:

i) Full name (including surname and given names consistent with applicable law and national identification practices); and

ii) Date and place of birth, or reference to at least one 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 identified in association with a legal person, additional evidence shall be provided of:

i) Full name and legal status of the associated organisational entity;

ii) Any relevant existing registration information (e.g. company registration) of the organisational entity; and

iii) Evidence that the Subject is affiliated with the organisational entity which may include reference to an attestation or a trusted register. Attestations may be made by directors, executives, board members, or a natural person with authorisation duly delegated from another natural person in an authorised role.

Delegated administrators at Enterprise RAs may assert an Applicant's affiliation with the organisational entity using the QuoVadis Certificate Management System is Certificmee

•	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.

2.4.3. QV Advanced +

Purpose

QuoVadis Advanced+ Certificates are used for the same purposes as Advanced Certificates, with the only difference being that they are issued on a Secure Cryptographic Device either held by the Subscriber or managed by QuoVadis. The QuoVadis Advanced+ Certificate Class is trusted in the Adobe Approved Trust List (AATL).

QVSwissQualified Certificates are Qualified personal certificates according to the Swiss Federal signature law (ZertES). They are issued out of the "QuoVadis Swiss Regulated CAs" and have the notice text "qualified certificate" in the Certificate Policies user notice. QVSwissQualified Certificates are used to sign documents electronically. The Digital Signature is tamperproof and legally equivalent to a handwritten signature.

Registration Process

QVSwissQualified Certificates are issued in accordance with the ZertES requirements using various QuoVadis Signing Services designed for this type of Certificate

i) Business SSL Certificates are Certificates for which limited authentication and authorisation checks are performed on the Subscriber and the individuals acting for the Subscriber (OID 1.3.6.1.4.1.8024.0.2.100.1.1)

ii) Extended Validation SSL Certificates

WHETHER QUOVADIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CPYCBESMMADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER.

- For Swiss Qualified Certificates, QuoVadis liability is in accordance with Articles 17, 18, 19 of ZertES.
- For EU Qualified Certificates, QuoVadis liability is in accordance with Extract 37 and Article 13 ofM,OT i BEEA

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

Signature, not the accuracy of the underlying electronic record. Relying Party Agreements may include additional representations and warranties.

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.

exclusive jurisdiction over any of the matters, claims or disputes contemplated in subsection (i) above, will each depend on where Customer is domiciled, as set forth in the table below.

In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be/4itnb]TJ 0t (r)-827

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 af 0.446 e-Hf 0.4aj(6.6 (aga.7 (en)446 e-H8 (d)-5n.7 (:)- .9 (7)-5.4 (h)3.e2 (ed)6.8 (u)3.8 (n)9.8 (d32.8 (,)-0. e pa d T* [(p (ou)- (u)-15.2 (ir-12 (r)3.4 7-12 of)-11.32.4 (r)da(1e-H (c)-5.5 (d d72 (l)-7.p (o7)7)-7 (q)3.)-7 (n)2.