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: 22

Version Control:

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

[redacted]

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 : DigiCert Bermuda Limited (previously QuoVadis Limited), Washington Mall 3F, 7 Reid Street, Hamilton HM-

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	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 tothe Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n-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 ODs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-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 (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: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
	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

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 Classes			
		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			

2.3. IDENTITY AUTHENTICATION

Base RIV includes OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options include read of eMRTD data, Passive Authentication, and Active Authentication.

2.4. CERTIFICATE CLASSES

2.4.1. QV Standard

htivp chtivamp2.14Tf 0.005-(A)-4.5031 pTf03 Tw 16(A)-4.35901 23 Tw 1Stop4ide and -6 Tw (8A))-4TJ -0.0s(A)-4..9(64(A)-1)0.7.83(R)-6.(et8 (

Purpose

-

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS.

Swiss Qualified Certificates issued under the Swiss Federal signature law (ZertES) also meet this ETSI policy QCP-n-qscd. These Swiss Qualified Certificates are issued only to natural persons out of the “QuoVadis Swiss Regulated CA G1” and have the notice text “qualified certificate” in the CertificatePolicies user notice.

The content of these Certificates meet the relevant requirements of:

- ETSIEN 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

details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA.

2.4.4.4. eIDAS

viii) Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, including only installing TLS/SSL Server Certificates on servers accessible at the Domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent; and

ix) Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that QuoVadis notifies the Subscriber that the QuoVadis PKI has been compromised.

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.
- ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted Lists. ETSI TS 119 172-4 describes how to validate a digital signature to determine whether it can be considered as an EU Qualified electronic signature or seal.

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

- the identity of the Subscriber is displayed correctly by utilising trusted application software; and
-

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. GOVERNING LAW

The (i) laws that govern the interpretation, construction, andenforcement of this Agreement and all matters,

Customer is Domiciled in or the Services are:	Governing Law is:	Court or arbitration body with exclusive jurisdiction:
A Country in Asia or the Pacific region, other than Japan, Australia or New Z5.6 (o2.5plan)9(o2.dTJ 0 Tc 0 Tw 10.16855 Td ( )Tj ET EMC /Ar<</MCID 11 3>BDC q 220.8 686.04		