DigiCert Europe / QuoVadis

PKI Disclosure Statement

Effective Date: 22 November, 2023
Version: 2.0

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement
QuoVadis PMA	15 June 2017	1.1	Based on ETSI TS319 411 model disclosure statement and eIDAS regulation
QuoVadis PMA	13 September 2017	1.2	Updates for submission of complaints.
QuoVadis PMA	20 August 2018	1.3	[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-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: DigiCert Deutschland GmbH (previously QuoVadis Trustlink Deutschland GmbH), Ismaninger Str. 52, D-81675 München, Germany. Phone: +48 (9)]TJ 0 Tc 0 [611.3 (1)0.7 (5)]TJ 0 Tc d4 w 0.807 0 Td [(Sg[(7)0.8 (9)]

in the CP/CPS may be drawn up under contract for individual customers. Please refer to the CP/CPS for the full details.

Please note that where the term "Qualified Certificate" is used in this document it is consistent with the definition of "Qualified Certificate" in ETSI EN 319 411-2 and Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation"). QuoVadis Qualified CAs are listed on the EU Trusted List (EUTL) for the Netherlands and for Belgium.

In the case of Qualified Certificates, where QuoVadis manages the keys on behalf of the Subscriber, QuoVadis shall require:

- where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures are only created by the QSCD;
- in the case of natural persons, the Subscriber's private key is maintained and used under their sole control and used only for electronic signatures; and
- in the case of legal persons, the private key is maintained and used under their control and used only for electronic seals.

2.1. QUOVADIS CERTIFICATE CLASSES

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
QV Standard	Based on the ETSI Lightweight Certificate Policy (LCP),which has the policy identifier OID 0.4.0.2042.1.3	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.100 (optional, may also use S/MIME BR OIDs) ETSI policy identifier OID: 0.4.0.2042.1.3 (optional)	Low	Optional
QV Advanced	Based on the ETSI Normalised Certificate Policy (NCP), which has the OID 0.4.0.2042.1.1. Features faee to-face (or equivalent) authentication of holder identity and organisational affiliation (if included).	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.200 ETSI policy identifier OID: 0.4.0.2042.1.1 (optional)	Medium	Optional
QV Advanced +	Similar to "QV Advanced" issued on an SSCD. Based on the ETSI Normalised Certificate Policy requiring an SSCD (NCP+), which has the OID 0.4.0.2042.1.2 Includes Swiss Regulated Certificates.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300 ETSI policy identifier OID: 0.4.0.2042.1.2 (optional)	High	Yes Adobe AATL Approved

Certificate Class	Description

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 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 recognised 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 another 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 Portal

By requesting a QuoVadis Certificate, an Applicant accepts to undertake one of the following identity proofing methods and the related terms and conditions. QuoVadis may provide alternative identity verification methods available to the relevant Certificate Class

- Physical.831 -1.(h)3.8 e to

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

2.4. CERTIFICATE CLASSES

2.4.1. QV Standard

Purpo(7)(g>BDC /TT0 1 Tf 9.96(36)2.7 (,)-12.8 ( )]TJ -0.)Tj /TT4 1 Tf 0 Tc 0 Tw 2.47 0 Td ( )Tj /TT3 1 T

•

Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands

QuoVadis QCP-w Certificates will be issued under the requirements of ETSI EN 319 411-2 and aim to support website authentication based on a Qualified defined in articles 3 (38) and 45 of the eIDAS Regulation.

QCP-w Certificates issued under these requirements endorse the requirement of EV Certificates whose purpose is specified in clause 5.5 of ETSI EN 319 411-2 [2]. In addition, EU Qualified Certificates issued under this policy may be used to provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website as specified in the eIDAS Regulation. The certificate profile below is designed in acc45TJ-T* [(T)1.61.9 B4.8 (9sIBDC 9.r9sIBt3.8 (y)-3 ( )- (4)0.8 (1)0.8 (5.687

Private Keys for QV Swiss Qualified Certificates are generated and stored on an HSM Hardware Security Module or USB token that meets the ZertES requirements, FIPS 140-2, level 3 or EAL 4 standards. HSMs for QuoVadis Signing Services are located in QuoVadis datacentres. Access by the Subscriber to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone SSCD.

QV Swiss Qualified Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour.

2.4.5.1. Swiss Regulated Certificate issued to a Natural Person

Purpose
Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ Certificate Class. They are issued out of Swiss Regulated CAs and have the notice text “regulated certificate” in the CertificatePolicies user notice
Registration Process
Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV ZERTES apply to the specification of Swiss Regulated Certificates. For the issuance and life cycle management of Swiss Regulated Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES Qualified Certificate.

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. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows establishment of [(Swiss) Government

Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.

These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or the obligations on the TSP managing the key on their behalf) are set out in clause 11.2.

of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CP/CPS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) QUOVADIS AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "QUOVADIS ENTITIES") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF; AND (B) THE QUOVADIS ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO QUOVADIS IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF 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 CP/CPS, MAY BE MADE 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 of the eIDAS Regulation.

4. OBLIGATIONS OF SUBSCRIBER

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify QuoVadis and any applicable RA if a change occurs that could affect the status of the Certificate.
QuoVadis requires, as part of the Subscriber Agreement or Terms

vi) For Remote Identity Verification, use the identity proofing software distributed by QuoVadis. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;

vii) Ensure that individuals using Certificates on behalf of an organisation have received security training appropriate to the Certificate;

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

- 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 been altered following signature by utilising trusted application software,
- the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
-

9. REFUND POLICY

QuoVadis or Issuing CAs under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements. See Section 9.1.5 of the CP/CPS

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. GOVERNING LAW

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-section (i) above, will each depend on where Customer is domiciled or, if the dispute arises from a PKIoverheid Certificate, as set forth in the table below; provided, for clarity

Customer is Domiciled in or the Services are:	Governing Law is:	Court or arbitration body with exclusive jurisdiction:
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, otherCougi6 77.4 618 676.44 f 72.24 622 Tw 9.96 -0 0 9.96 77.4 618.84 Tm [(r)3.4 (e)-7 (g)-1 (ion)2.8 (,)-12.9 (oth	seat of arbitration in Melboue	