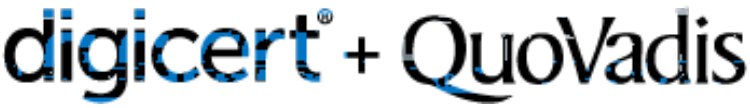
QuoVadis

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:	March 27, 2020
Version:	1.8

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 Subscriberand Relying Parties.

This document does not substitute or replace the Certificate Policy/Certification Practice Statement (CP/CPS) under which Digital 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 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 p(r)5d(6.9 (te.3 ( ) 4.59 0 Td (r)3.4 l1 (a)-6.0.001 T.4 (ti)-125TjETEMt

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	Updates for Qualified Website Authentication Certificates and link to Privacy Notice.
QuoVadis PMA	30 august 2018	1.4	Update for Qualified website authentication certificates information
QuoVadis PMA	7 December 2018	1.5	

TABLE OF CONTENTS

QuoVadis Certificate Class	Description	QuoVadis / ETSI Certificate Policy OID	Assurance Level	Requires token?
	qscd), with the OID 0.4.0.194112.1.2 • EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the policy identifier OID 0.4.0.194112.1.3			
	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. • May include PSD2 fields	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

2.3. QV STANDARD

Purpose
Standard Digital 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 Digital 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.

2.4. QV ADVANCED

Purpose
QV Advanced Digital Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, 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 has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Subscriber shall include the following: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. If the subject is a natural person 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. If the subject is a natural person who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. If the Subscriber is a natural person who is identified in association with a legal person (organisational entity), additional evidence shall be provided of: • Full name and legal status of the associated legal person; • Any relevant existing registration information (e.g. company registration) of the associated legal person; and • Evidence that the Subscriber is affiliated with the legal person. If the Subscriber is a legal person (organisational entity), evidence shall be provided of: • Full name of the legal person; and • 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. If the Subscriber is a device or system operated by or on behalf of a legal person, evidence shall be provided of:

- identifier of the device by which it may be referenced (e.g. Internet domain name);
- full name of the organisational entity;
- a nationa

- 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.

If the Subscriber is identified in association with an organisational entity, additional evidence shall .009 To1.9 ()-15.t1.9 ()-1

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 PUB 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 assu.( )]T(y) Tc 0 Tw 34.181 07.904-n.48(n.48(ref7714 719.5[(n.48(n.48(ref77181 719.5[(

- 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 may be provided on behalf of the subject by the RA. However, the subject remains responsible for the content of the Certificate.

If the Subscriber is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Subscri7 (c)-5a r7 (r) e RA2 thic4h t thergan2istional(a)-6.9 (n)2.8 (ti3-6.9 (.)]TJ0 Tc 0Tw 048.217 c 2(5-4S) t.

The content of these Certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

Registration Process

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for "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).

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence by an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which QuoVadis can prove the equivalence. The

2.6.4. eIDAS Qualified Certificate issued to a Legal Person

Purpose
The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation. These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person" (QCP-l). QuoVadis recommends that QCP-l certificates are used only for electronic seals. The content of these certificates meet the relevant requirements of: • ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures • ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons • ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements • ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

Registration Process

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person" (QCP-l).

The registration process for these Certificates is the same as for the QCP-l-qcsd Certificates described in 2.6.3 above. The only difference is that these QCP-l certificates do not use a QSCD for the protection of the private key.

-

QCP-w-PSD2 Certificates include additional information in accordance with ETSI TS 119 495 describing the PSP roles, Authorisation Number, and NCA. The registration process for this PSD2 information is the same as for the QCP-l-qcsd Certificates described in 2.6.3 above.

2.7. CLOSED COMMUNITY CERTIFICATES

Closed Community Issuing CAs can, under contract, create Certificate Profiles to match the QuoVadis Standard Commercial Certificate for issuance to employees and affiliates.

Certificates issued by Closed Community Issuing CAs f3-4.MAs f3ialanced 9ymembe is tua c7-4.3 (ommu3a)-7-9uytionlyt,

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 SUBSCRIBERS

Digital Subscribers are required to act in accordance with the CP/CPS and the relevant Subscriber/Subscriber Agreement. A Digital Subscriber represents, warrants and covenants with and to QuoVadis, Relying Parties, Application Software Vendors and the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Subscriber, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing CA, Registration Authority, or QuoVadis immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorised viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorised use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Subscriber's Public Key. In the case of legal persons, the private key must be maintained and used under the control of the Subscriber and is recommended to be used only for electronic seals.
- If the policy requires the use of a Qualified Electronic Signature Creation Device (QSCD), digital signatures must only be created by a QSCD.
- For Qualified certificates issued to natural persons, it is recommended that the Subscriber's key pair is only used for electronic signatures.
- Immediately notify the Issuing CA, Registration Authority or QuoVadis in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever. Following compromise, the use of the Subscriber's Private Key should be immediately and permanently discontinued. For certificates issued from the itsme sign Issuing CA G1 all revocation requests must be directed to the itsme first-line helpdesk.

•

Customer is Domiciled in:	Governing Law is laws of:	Court or arbitration body with exclusive jurisdiction:
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah M.3 (3(t (e) (3(tni06 Tw Tc.3 (de)C 71.7(

class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

- For Swiss Qualified Certificates such arbitration shall, unless agreed otherwise between the parties, take place in Switzerland.
- For Qualified Certificates issued in accordance with eIDAS, arbitration for disputes related to financial or commercial matters will be dealt with in the country of the relevant QuoVadis entity named in the contract with the client. Arbitration for Certificate-related disputes will be dealt with in the country named in relevant QuoVadis Issuing CA Certificate.

11. CA AND REPOSITORY