PKI DISCLOSURE STATEMENT

Effective Date: 15 June 2017
Version: 1.1

Important Notice about this Document

This document is the PKI Disclosure Statement herein after referred to as the PDS. This document does not substitute or replace the Certificate Policy/Certification Practice Statement (CP/CPS) under which digital certificates issued by QuoVadis Limited (QuoVadis) are issued. You must read the CP/CPS at www.quovadisglobal.com/repository before you apply for or rely on a Certificate issued by QuoVadis.

The purpose of this document is to summarise the key points of the QuoVadis CP/CPS for the benefit of Subscribers, Certificate Holders and Relying Parties.

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 pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business. This version of the PDS has been approved for use by the QuoVadis Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA. The date on which this version of the PDS becomes effective is indicated on this document.

Version Control:

Author	Date	Version	Comment

1. CA CONTACT INFO

Bermuda and Group
Corporate Offices:
QuoVadis Limited
3rd Floor

2.5 QV Advanced +

PURPOSE

QuoVadis Advanced+ Digital Certificates are used for the same purposes as QuoVadis Advanced Digital Certificates, with the only difference being that they are issued on a Secure Cryptographic Device. The QuoVadis Advanced+ Certificate ClasET7.8 reW*n ClasET7.8 reW*n ClasET7.8 reW*n C$es aeG7.38 Tmh5 461.0 1 83.eW*b12(g)6(i1.0 18 T

2.5.2 SuisseID Identity and Authentication Certificates

PURPOSE

2.6 QV Qualified

2.6.1. eIDAS Qualified Certificate issued to a natural person on a QSCD

PURPOSE

The purpose of an EU Qualified certificates is to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by Regulation (EU) No. 910/2014 on electronic identification and trust serv19qG -0.pe for electronic transactions in the internal market (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 natural person where the private key and the related certificate reside on a QSCD (QCP-n-qscd).(

2.6.2 eIDAS Qualified Certificate issued to a natural person

PURPOSE

The purpose of these EU Qualified certificates are to identify the Certificate Holder with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.

This type of QuoVadis Qualified certificates does not use a QSCD for the protection of the private key.

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 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

REGISTRATION PROCESS

The identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for the “Policy for EU qualified certificate issued to a natural person” (QCP-n). The registration process for these certificates is the same as for the QCP-n-qcsd Certificates described in 2.5.1 above. The only difference is that these QCP-n certificates do not use a QSCD for the protection of the private key.

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 Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person

anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. QuoVadis verifies that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used

4. OBLIGATIONS OF SUBSCRIBERS

Digital Certificate Holders are required to act in accordance with the CP/CPS and the relevant Certificate Holder/Subscriber Agreement. A Digital Certificate Holder 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 Certificate Holder, 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 Certificate Holder's Public Key.

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 Certificate Holder's Private Key should be immediately and permanently discontinued.

Take all reasonable measures to avoid the compromise of the security or integrity of the QuoVadis PKI.

Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.

At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.

Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.

Discontinue the use of the digital signature Key Pair in the event that QuoVadis notifies the Certificate Holder that the QuoVadis PKI has been compromised.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to be an Authorised Relying Party, a Party seeking to rely on a Digital Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement (www.quovadisglobal.com/repository) by querying 510047>-8<0003>-1

6. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation,

10.2 Dispute Resolution

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a “participant” within the QuoVadis PKI) arising out of or relating to the QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.

Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.

Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing 0 1 97.344 569.62 Tm0 g0 G[(s)6(uing)-8( )6(0 1 97.344 569.62 Tm0 g 9 Tf1 0 0 1 97.344 569.62 Tm0 g0 G[(s)6(uing)-8(