PKI DISCLOSURE STATEMENT

Effective Date: 27 May 2008
Version: 1.0

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
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement

Table of Contents

1. CA CONTACT INFO 1
2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE 1
2.1 Standard Test Certificate 1
2.2 Standard Personal Certificate 2
2.3 Qualified Certificate 2
2.4 Standard Commercial Certificate 3
2.5 Commercial - ElDI-V Certificates 3
2.6 Special Purpose Certificates 3
2.7 Closed Community Certificates 4
2.8 SSL and Code Signing Certificates 4
3. RELIANCE LIMITS 5
4. OBLIGATIONS OF SUBSCRIBERS 5
5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES 6
6. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY 6
7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT CERTIFICATE POLICY 6
8. PRIVACY POLICY 7
9. REFUND POLICY 7
10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION 7
10.1 Governing Law 7
10.2 Dispute Resolution 7
11. CA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT 7

1. CA CONTACT INFO

Bermuda and Group

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11,
Bermuda
Phone: +1-441-278-2800
Website: www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

Mailing Address:
QuoVadis Limited
Suite 1640
48 Par-La-Ville Road
Hamilton HM-11
Bermuda

Netherlands
QuoVadis Trustlink BV
Maliesingel 22
3581 BG Utrecht
The Netherlands
Phone: +31 (0) 30 232-4320

Switzerland
QuoVadis Trustlink Schweiz AG
Teufenerstrasse 11
9000 St. Gallen
Switzerland
Phone: +41-71-272-60-60

United Kingdom
QuoVadis Online Security Limited
8 Hayters Court, Brockenhurst Business Park
Grigg Lane, Brockenhurst
Hampshire SO42 7PG
United Kingdom
Phone: +44 (0) 1590-624400

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. The procedures for Digital Certificate Holder registration and validation are described below for each type of Digital Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described below or in the CP/CPS may be drawn up under contract for individual customers.

Please note that where the term "Qualified Certificate" is used in this document it is consistent with the definition of "Qualified Certificate" in ETSI TS 101 456 and the European Union Directive 1999/93/EC.

2.1 Standard Test Certificate

INITIAL REGISTRATION
• Issued by approved Issuing CAs in the QuoVadis PKI. • Registration performed by approved Registration Authorities in the QuoVadis PKI.
IDENTIFICATION & AUTHENTICATION
There is no formal Identification & Authentication requirement for Standard Test Digital Certificates. Standard Test Digital Certificates are issued for limited duration on the basis of the Applicant Digital Certificate Holder's self certification.
REGISTRATION PROCESS
Registration information may be received from an Applicant Digital Certificate Holder: • In person, or • By mail or electronic methods

Standard Test Digital Certificates Holders participate in the QuoVadis PKI. Issued to Digital Certificate Holders based on non-certified forms of identification; designated as a No-Reliance Digital Certificate. A Registration Authority Officer collects Digital Certificate Holder details during the Application process ensuring that the information supplied is correct. During the registration process, it is a requirement for an Applicant Digital Certificate Holder to accept the Certificate Holder agreement. The Certificate Holder Agreement details the terms and conditions under which the Digital Certificate is being supplied including the Digital Certificate Holder's rights and obligations.

2.2 Standard Personal Certificate

INITIAL REGISTRATION

- Issued by the QuoVadis Issuing CA.
- Registration performed by QuoVadis Registration Authorities.

IDENTIFICATION & AUTHENTICATION

Accredited Digital Certificate under the Bermuda Certification Service Provider Legislation, issued to Applicant Digital Certificate Holders based on the in-person presentation of required identification to a QuoVadis Registration Authority.

REGISTRATION PROCESS

A QuoVadis Registration Authority Officer verifies that the Government issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (*e.g.,* holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:

- in person or
- by mail or electronic methods.

The Registration and Authentication process of a Standard Personal Digital Certificate Holder's identity includes:

- the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.
- one form of government issued photographic identification is reviewed and photocopied.
- one additional form of identification, the name on which corresponds to the name that appears on the government issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.

2.3 Qualified Certificate

Please note that where a Qualified Personal Digital Certificate is issued within the meaning of EU Directive 1999/93/EC, the individual applying for the Qualified Personal Digital Certificate must undergo a face-to-face identity verification procedure.

INITIAL REGISTRATION

- Issued by QuoVadis Issuing CA.
- Registration performed by a QuoVadis Registration Authorities.

IDENTIFICATION & AUTHENTICATION

The purpose of a Qualified Personal Digital Certificate is to identify a person with a high level of assurance, where the Qualified Personal Digital Certificate meets the qualification requirements defined by the applicable legal framework of the European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

REGISTRATION PROCESS

A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (*e.g.,* holographic devices). The applicant certificate holder must present original documentation in person during a face-to-face verification procedure.

The Registration and Authentication process of a Qualified Personal Digital Certificate Holder's identity includes:

- the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority with either a valid Passport or Government-issued Identification Card.
- one form of government-issued photographic identification is reviewed and photocopied.
- one additional form of identification, the name on which corresponds to the name that appears on the government-issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.
- All information on the applicant form and all certificate fields shown in the certificate are verified as accurate.

2.4 Standard Commercial Certificate

INITIAL REGISTRATION

- Issued by approved Issuing CAs in the QuoVadis PKI.
- Registration performed by approved Registration Authorities in the QuoVadis PKI.

IDENTIFICATION & AUTHENTICATION

Accredited Digital Certificate under the Bermuda Certification Service Provider Legislation, issued to Applicant Digital Certificate Holders based on the applying Certificate Holder's contractual relationship to the company that operates the Nominating Registration Authority, or its respective subsidiaries and holding companies.

REGISTRATION PROCESS

A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (*e.g.,* holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:

- in person or
- by mail or electronic methods.

The Registration and Authentication process of a Standard Commercial Digital Certificate Holder's identity includes:

- the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.
- one form of government-issued photographic identification is reviewed and photocopied.
- one additional form of identification, the name on which corresponds to the name that appears on the government issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.

2.5 Commercial - ElDI-V Certificates

A Commercial Advanced Certificate enables an authorised person or a commercial entity directly associated with a secure signature creation device in conformity with ElDI-V (SR 641.201.1 and SR 641.201.1.1) to digitally sign with the Secure Signature Creation Device (SSCD). The procedure below assumes an application by a company or organisation on behalf of its employees or devices for Digital Certificates.

INITIAL REGISTRATION

- Issued by QuoVadis Issuing CA.
- Registration performed by a QuoVadis Registration Authority.

PURPOSE

The purpose of a Commercial Advanced Digital Certificate is to identify the organisation and individual responsible for creation of signatures under SR 641.201.1 and SR 641.201.1.1.

REGISTRATION PROCESS

A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (*e.g.,* holographic devices). The applicant certificate holder must present original documentation in person during a face-to-face verification procedure.

The Registration and Authentication process of a Qualified Commercial Digital Certificate Holder's identity includes:

The Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority with either a valid Passport or Government-issued Identification Card.

During the Registration process one form of government issued photographic identification is reviewed and photocopied and one additional form of identification, the name on which corresponds to the name that appears on the government-issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.

All information on the applicant form and all certificate fields shown in the certificate are verified as accurate.

For a commercial entity, (company, partnership, sole trader etc.) The Registration Authority must seek positive assurance regarding the details listed in the certificate by reference to the appropriate official register for that company type.

2.6 Special Purpose Certificates

INITIAL REGISTRATION

- Issued by QuoVadis Issuing Certification Authority.
- Registration performed by a QuoVadis Registration Authority.

DESCRIPTION
Special Purpose Digital Certificates include certificates issued primarily for one or more of the Extended Key Usages as shown below. These certificates may be issued to natural persons, devices or organisations.
REGISTRATION PROCESS
An application form for a Special Purpose Digital Certificates is submitted, defining the contents of the fields required to be completed. For: • Natural person: a copy of an official photo ID document with signature or the confirmation of a notary or other accredited third party regarding the correctness and the completeness of the data is required. Where applicable, the affiliation of a person named in a certificate to a stated organization must be confirmed by an authorized member of that organization, which may be verified by phone. • E-mail address: the correctness is verified by an access test or by confirmation from the organization with which the individual is associated. • Organizations are verified by presentation of a copy of a document, which proves the existence of the organization, or by verification from an official register. • Device details: confirmation of device serial number or other unique identifying mark sought by the applicant. • Where an applicant requests a Code Signing Certificate, that applicant must confirm that the application details they provide are truthful, accurate, and not misleading, (application name, information URL, and application description). The Certificate Holder also must be identified by a verified organization name. Failure by a subscriber to comply, or to promptly correct inaccurate information should result in revocation of the code signing certificate. QuoVadis will revoke certificates issued to subscribers who use it to digitally sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

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 are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone certificate policy to its community issue various certificates that differ from the Standard Commercial Certificate.

QuoVadis must approve all closed community certificate policies to ensure that they do not conflict with the terms of the QuoVadis CP/CPS.

Under no circumstances can Closed Community Issuing CAs issue Qualified Certificates under European Digital Signature law.

2.8 SSL and Code Signing Certificates

QuoVadis issues three forms of Certificates according to the terms of the QuoVadis Root CA2 CP/CPS (www.quovadisglobal.com/repository):

i. Business SSL Certificates are Certificates for which limited authentication and authorization checks are performed on the Subscriber and the individuals acting for the Subscriber.

ii. Extended Validation SSL Certificates are Certificates issued in compliance with the “Guidelines for the Issuance and Management of Extended Validation Certificates” (EV Guidelines) published by the CA/Browser Forum. The EV Guidelines are intended to provide enhanced assurance of identity of the Subscriber by enforcing uniform and detailed validation procedures across all EV-issuing CAs.

iii. Trusted Code Signing Certificates are Certificates issued in compliance with Code Signing Certificate Guidelines, including identification of the Certificate Holder by a verified organization name and certificate revocation for any misrepresentation or publication of malicious code.

3. RELIANCE LIMITS

Refer to section 9.8 of the CP/CPS (www.quovadisglobal.com/repository) for reliance limits. QuoVadis' liability for breach of its obligations pursuant to the QuoVadis CP/CPS shall, in the absence of fraud or wilful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below:

Loss Limits / Reliance Limits	Maximum per Certificate
Standard Certificates	US$250,000
Device Certificate	US$250,000

In no event shall QuoVadis' liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular Digital Certificate to the intent that the loss limits reflect QuoVadis' total potential cumulative liability per Digital Certificate per year (irrespective of the number of claims per Digital Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Digital Certificate in any one year of that Digital Certificate's life cycle.

According to Digital Signature law (including ZertES, TAV SR 943.032.1 and ETSI TS 101 456) the only appropriate use for Qualified Digital Certificates is signing.

All events involved in the generation of the CA key pairs are recorded. This includes all configuration data and registration information used in the process. Audit logs are retained as archive records for a period no less than eleven (11) years for audit trail files, and no less than eleven (11) years for Key and Digital Certificate information.

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 Digital 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.
- 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.
- 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 Digital Certificate Holder.
- Discontinue the use of the digital signature key pair in the event that QuoVadis notifies the Digital Certificate Holder that the QuoVadis PKI has been compromised.

- For Qualified Certificates, private keys are generated on a Secure Signature Creation Device (SSCD) in the presence of the Certificate Holder. The individual applying for the Qualified Certificate must undergo a face-to-face identity verification procedure. The Certificate Holder is responsible for directly securing the SSCD with a Personal Identification Number.

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 the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

Authorised Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Digital Certificate for any given purpose and that the use is not prohibited by the CP/CPS.
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.
- That the Digital Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List (http://crl.quovadisglobal.com/<caname>.crl) or is made available via Online Certificate Status Protocol checking (http://ocsp.quovadisglobal.com) where available.

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, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment (save as may arise directly from breach of the CP/CPS), wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis’ liability to any person for damages arising under, out of or related in any way to the CP/CPS, Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. QuoVadis shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the QuoVadis PKI (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the QuoVadis PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon the foregoing as a condition and inducement to permit that person to participate within the QuoVadis PKI.

Refer to the CP/CPS (www.quovadisglobal.com/repository) for further detail as to liability and warranties.

7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT CERTIFICATE POLICY

The following documents are available online at www.quovadisglobal.com/repository:

- Certificate Policy/Certification Practice Statement
- End User Certificate Holder Agreement
- SSL Certificate Subscriber Agreement

- Code Signing Certificate Subscriber Agreement
- Digital Certificate Terms and Conditions of Use
- Relying Party Agreement

8. PRIVACY POLICY

Data contained within a QuoVadis Certificate is considered public information. Personal data obtained during the registration process will not be released without prior consent of the relevant certificate holder, unless required otherwise by law or to fulfil the requirements of the CP/CPS. Refer to the QuoVadis Privacy Statement at http://www.quovadisglobal.com/privacy.aspx.

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. Refer to section 9.1.5 of the CP/CPS (www.quovadisglobal.com/repository).

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1 Governing Law

Subscribers and Relying Parties shall use QuoVadis Certificates and any other related information and materials provided by QuoVadis only in compliance with all applicable laws and regulations. QuoVadis may refuse to issue or may revoke Certificates if, in the reasonable opinion of QuoVadis, issuance or the continued use of the QuoVadis Certificates would violate applicable laws or regulations.

QuoVadis Certificates issued by QuoVadis are governed by the laws of the country referred to in the Subscriber Agreement for the Certificate in question, without reference to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods.

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 CA.

For Qualified Certificates issued in accordance with Swiss Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in Switzerland. For Qualified Certificates issued in accordance with Dutch Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in The Netherlands.

11. CA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

In the provision of Trust Services, QuoVadis maintains several accreditations and certifications of its Public Key Infrastructure. These include:

- **WebTrust for Certification Authorities**. The WebTrust seal of assurance for Certification Authorities symbolises to potential relying parties that a qualified practitioner has evaluated the Certification Authority's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities, and has issued a report with an unqualified opinion indicating that such principles are being followed. This audit is performed on an annual basis by Ernst & Young.

- **Qualified Certification Service Provider (Switzerland)**. QuoVadis is entitled to issue and administer qualified electronic certificates in accordance with Swiss law. This includes certification to SR 943.03 (ZertES), ETSI TS 101.456 (Policy requirements for Digital Certification Authorities issuing Qualified Digital Certificates) and other standards. This audit is performed on an annual basis by KPMG.

- **Authorised Certification Service Provider (Bermuda).** QuoVadis is entitled to issue accredited certificates under the requirements of the Bermuda Electronic Transactions Act 1999.