QUOVADIS ROOT CERTIFICATION AUTHORITY
CERTIFICATE POLICY /
CERTIFICATION PRACTICE STATEMENT

OIDs: 1.3.6.1.4.1.8024.0.1
1.3.6.1.4.1.8024.0.3

Effective Date: 29 October 2007

Version: 4.4

Important Note About this Document

This is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited, (QuoVadis). It contains an overview of the practices and procedures that QuoVadis employs as a Certification Authority (CA). This document is not intended to create contractual relationships between QuoVadis Limited and any other person. Any person seeking to rely on Digital Certificates or participate within the QuoVadis Public Key Infrastructure (the QuoVadis PKI) must do so pursuant to a definitive contractual document. This document is intended for use only in connection with QuoVadis and its business. This version of the CP/CPS 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 and as otherwise set out herein. The date on which this version of the CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

This document covers aspects of the QuoVadis PKI that relate to all CAs established by QuoVadis under the QuoVadis Root Certification Authority and the QuoVadis Root Certification Authority 3 (QuoVadis Root CA 3). There are a number of instances where the legal and regulatory framework regarding the issuance of Qualified Certificates under either the Swiss or European Digital Signature regimes require deviation from QuoVadis standard practices. In these instances, this Document shows these differences either by indicating in the body of the text "For Qualified Certificates" or with the inclusion of a Text Box as follows:

> This is a provision specifically about Qualified Certificates.

Contact Information:

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11,
Bermuda

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

Website: www.quovadis.bm
Electronic mail: policy@quovadis.bm

Version Control:

Author	*Date*	*Version*	*Comment*
QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	WebTrust Revisions
QuoVadis PMA	01 April 2004	2.07	WebTrust Revisions
QuoVadis PMA	11 November 2005	2.08	WebTrust Revisions
QuoVadis PMA	17 April 2006	4.00	Cumulative ZertES Revisions
QuoVadis PMA	14 September 2006	4.1	EIDI-V Certificate Requirements
QuoVadis PMA	26 February 2007	4.2	QuoVadis Root CA 3 Added
QuoVadis PMA	03 April 2007	4.3	Clarifications to Appendix A
QuoVadis PMA	29 October 2007	4.4	General Edits and RFC3647 Conformity, Cumulative ZertES and ElDI-V Revisions

1. INTRODUCTION

1.1. Overview

This QuoVadis CP/CPS sets out the policies, processes and procedures followed in the generation, issue, use and management of Key Pairs and Digital Certificates. It also describes the roles, responsibilities and relationships of participants within the QuoVadis PKI.

This CP/CPS outlines the trustworthiness and integrity of the QuoVadis Root CAs' operations. A fundamental concept underpinning the operation of the QuoVadis PKI is trust. Trust must be realised in each and every aspect of the provision of Certification Services and Operations including Digital Certificate Holder applications, issuance, renewal, revocation or expiry.

With the exception of Certification Authorities issuing Qualified Certificates in accordance with Swiss Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing Certification Authority and Registration Authority services within the QuoVadis PKI.

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

- Authorised Certification Service Provider (Bermuda) entitled to issue accredited certificates under the requirements of the Electronic Transactions Act 1999. This authorisation synthesises elements of the ISO 17799 Code of Practice for Information Security Management and the European Electronic Signature Standardisation Initiative, as well as the WebTrust for Certification Authorities programme.

- WebTrust for Certification Authorities, conducted by Ernst & Young. This audit is consistent with standards promulgated by the American National Standards Institute, the Internet Engineering Task Force, and other bodies. It references the ANSI X9.79 Public Key Infrastructure Practices and Policy Framework (X9.79) standard for the financial services community and the American Bar Association's Public Key Infrastructure Assessment Guidelines.

- Qualified Certification Service Provider (Switzerland) en

1.2. Document Name, Identification and Applicability

The Private Enterprise Object Identifier (OID) assigned by the Internet Assigned Numbers Authority to QuoVadis is 1.3.6.1.4.1.8024.

The Object Identifier assigned for the certificate policy extension for certificates issued under the QuoVadis Root Certification Authority Certificate is 1.3.6.1.4.1.8024.0.1, while the OID assigned by QuoVadis for certificates issued under the QuoVadis Root CA 3 Certificate is 1.3.6.1.4.1.8024.0.3. These are used as the OID arcs for QuoVadis to identify the Certificate Policies under which it issues certificates pursuant to this CP/CPS:

QuoVadis Root Certification Authority	1.3.6.1.4.1.8024.0.1
QuoVadis Root CA 3	1.3.6.1.4.1.8024.0.3

The certificate policy extension in certificates issued in accordance with this CP/CPS shall assert at least one of these

QuoVadis provides identification and authentication services for Digital Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this CP/CPS and in Appendix A define the credentials necessary to establish the identity of an individual or entity.

For Qualified Digital Certificates according to the Swiss Digital Signature Law, all identification processes for individuals require applicants to present themselves for face-to-face verification.

QuoVadis has established the QuoVadis Root Certification Authority under which a number of subordinate services operate. These subordinate services within the QuoVadis PKI are either:

- managed and operated by QuoVadis; or
- managed by clients but operated by QuoVadis (outsourced services); or
- managed and operated by clients (external services).

This CP/CPS describes all subordinate services that operate under the QuoVadis Root Certification Authority, i.e. that are within the QuoVadis "chain of trust".

Participants ("Participants") within the QuoVadis PKI include:

- Certification Authorities

- Registration Authorities
- Digital Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance
- Authorised Relying Parties

The practices described or referred to in this CP/CPS:

- accommodate the diversity of the community and the scope of applicability within the QuoVadis chain of trust; and
- adhere to the primary purpose of the CP/CPS, of describing

- 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.
- 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.
- 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.

1.3.3.2. Accepted Limitation Of Liability

Digital Certificates include a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this CP/CPS. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

1.3.4. Relying Parties

Authorised Relying Parties are Individuals or Organisations who are authorised by contract to exercise Reasonable Reliance on Digital Certificates in accordance with the terms and conditions of this CP/CPS.

1.3.4.1. Obligations and Responsibilities

Authorised Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement.

An Authorised Relying Party must utilise Digital Certificates and their corresponding Public Keys only for authorised and legal purposes and only in support of transactions or communications supported by the QuoVadis PKI.

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance and that Authorised Relying Party is otherwise in compliance with the terms and conditions of their Relying Party Agreement. Any such Reliance is made solely at the risk of the Relying Party.

1.3.4.2. Reasonable Reliance

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance (as set out below) and that Authorised Relying Party is otherwise in compliance with the terms and conditions of the Authorised Relying Party Agreement and this CP/CPS. For the purposes of this CP/CPS and Relying Party Agreement, the term "Reasonable Reliance" means:

- that the attributes of the Digital Certificate relied upon are appropriate in all respects to the reliance placed upon that Digital Certificate by the Authorised Relying Party including, without limitation to the generality of the foregoing, the level of Identification and Authentication required in connection with the issue of the Digital Certificate relied upon.
- that the Authorised Relying Party has, at the time of that reliance, used the Digital Certificate for purposes appropriate and permitted under this QuoVadis CP/CPS ;
- that the Authorised Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Authorised Relying Party;

- that the Digital Certificate intended to be relied upon is valid and has not been revoked, the Authorised Relying Party being obliged to check the status of that Digital Certificate utilising either the QuoVadis Database, the QuoVadis Certificate Revocation List, or the QuoVadis Online Certificate Status Protocol and otherwise in accordance with the provisions of this QuoVadis CP/CPS ;
- that the Authorised Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- that the Authorised Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Digital Certificate being relied upon.
- that the Authorised Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
- that the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
- that the identity of the Digital Certificate Holder is displayed correctly by utilising trusted application software; and
- that any alterations arising from security changes are identified by utilising trusted application software.

1.3.4.3. Accepted Limitation Of Liability

Digital Certificates include a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this CP/CPS. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers.

1.3.4.4. Assumptions About A Certificate Holder

A relying party shall make no assumptions about information that does not appear in a Digital Certificate.

1.3.4.5. Certificate Compromise

A party cannot rely on a Digital Certificate issued by QuoVadis if the party has actual or constructive notice of the compromise of the Digital Certificate or its associated Private Key. Such notice includes but is not limited to the contents of the Digital Certificate and information incorporated in the Digital Certificate by reference, which includes this CP/CPS and the current set of revoked Digital Certificates published by QuoVadis--certificates have pointers to

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The QuoVadis Repository serves as the primary repository. However, copies of the X.500 Directory may be published at such other locations as are required for the efficient operation of the QuoVadis PKI.

2.2. Publication of Certificate Information

The QuoVadis Root Certification Authority and chained Issuing CAs publish a Repository that lists all Digital Certificates issued and all the Digital Certificates that have been revoked. The location of the repository and Online Certificate Status Protocol responders are given in the individual Certificate Profiles more fully disclosed in Appendix A to this CP/CPS.

2.3. Time or Frequency of Publication

Digital Certificate information is published promptly following generation and issue and within 20 minutes of being revoked.

2.4. Access Controls on Repositories

Read-only access to Repositories is available to Relying Parties twenty-four hours per day, seven days per week, except for reasonable maintenance requirements, where access is deemed necessary. Queries to the Repository must specify individual certificate information. QuoVadis is the only entity that has write access to Repositories.

3. IDENTIFICATION AND AUTHENTICATION

QuoVadis implements rigorous authentication requirements to ensure that the identity of the Digital Certificate Holder is proven. This may include face-to-face identity verification at the beginning of the Digital Certificate request procedure or at some point prior to Digital Certificate delivery to the Digital Certificate Holder. The registration procedure will depend on the type of Digital Certificate that is being applied for.

Issuing CAs may perform the Identification and Authentication required in connection with the issue of Digital Certificates, or they may delegate the responsibility to one or more Registration Authorities. The level of Identification and Authentication depends on the class of Digital Certificate being issued. See Appendix A for Digital Certificate profiles and the relevant Identification and Authentication requirements.

3.1. Naming

3.1.1. Types Of Names

All Digital Certificate Holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The QuoVadis Root Certification Authority approves naming conventions for the creation of distinguished names for Issuing CA applicants. Different naming conventions may be used by different Issuing CAs.

The Subject Name of all Digital Certificates issued to Individuals shall be the authenticated common name of the Digital Certificate holder. Each User must have a unique and readily identifiable X.501 Distinguished Name (DN). The

For Qualified Certificates issued according to the Swiss Digital Signature law, all fields containing information must be verified by the appropriate Registration Authority by reference to appropriate documentation and face-to-face presentation of Government-Issued ID or Passport.

3.1.2. Need For Names To Be Meaningful

Distinguished Names must be meaningful, unambiguous and unique. Pseudonymous names may be used. QuoVadis supports the use of Digital Certificates as a form of identification within a particular community of interest.

The contents of the Digital Certificate Subject Name fields must have a meaningful association with the name of the Individual, Organisation, or Device. In the case of Individuals, the name should consist of the first name, last name, and any middle initial. In the case of Organisations, the name shall meaningfully reflect the legal name or registered domain name of the Organisation or the trading or business name of that Organisation. In the case of a Device, the name shall state the name of the Device and the legal name or registered domain name of the Organisation responsible for that Device.

3.1.3. Pseudonymous Certificate Holders

QuoVadis Registration Authorities, their Subsidiaries or Holding Companies

3.2.2. Authentication Of Organisation Identity

The Identity of an Organisation is required to be Authenticated with respect to each Digital Certificate that asserts (i) the Identity of an Organisation; or (ii) an Individual or Device's affiliation with an Organisation. Without limitation to the generality of the foregoing, the Identity of any Organisation that seeks to act as a Registration Authority for its employees and/or employees of its respective Subsidiaries, Holding Companies or Counterparties is required to be Authenticated.

In order to Authenticate the Identity of an Organisation, at a minimum, confirmation is required that: (i) the

3.2.6. Criteria For Interoperation

The QuoVadis PKI operates in accordance with open standards under the x.509 criteria and as such Digital Certificates issued by the QuoVadis Issuing CA are fully interoperable with Digital Certificates issued by other Issuing

Appendix A) and the relevant Certificate Holder Agreement or other terms and conditions upon which the Digital Certificate is to be issued. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

4.1.2. Enrolment Process And Responsibilities

Certain information concerning applications for Digital Certificates is set out in this QuoVadis CP/CPS. However, the issue of Digital Certificates by Issuing CAs will be pursuant to forms and documentation required by that Issuing CA. Notwithstanding the foregoing, the following steps are required in any application for a Digital Certificate: (i) Identity of the Holder or Device is to be established in accordance with Appendix A, (ii) a Key Pair for the Digital Certificate is to be generated in a secure fashion, (iii) the binding of the Key Pair to the Digital Certificate shall occur as set forth in this CP/CPS, and (iv) the Issuing CA shall enter into contractual relations with the Certificate Holder for the use of that Digital Certificate and the QuoVadis PKI.

Each Issuing CA may adopt its own application forms and procedures, which Applicants will be required to satisfy. Each Holder of a Digital Certificate is required to be bound by contract with respect to the use of that Digital Certificate. These contracts may be directly between the Issuing CA and the Holder or imposed upon that Holder through terms and conditions binding upon him or her. All agreements concerning the use of, or reliance upon, Digital Certificates issued within the QuoVadis PKI must incorporate by reference the requirements of this QuoVadis CP/CPS as it may be amended from time to time.

4.2. Certificate Application Processing

4.2.1. Performing Identification And Authentication Functions

See Appendix A for Identification and Authentication requirements for each Digital Certificate profile.

4.2.2. Approval Or Rejection Of Certificate Applications

A Registration Authority will approve or reject Digital Certificate Holder applications based upon the Digital Certificate Holders meeting the requirements of this CP/CPS and the Digital Certificate Profiles contained in Appendix A.

QuoVadis, at its sole discretion not to be unreasonably withheld, may override any decision to Approve a Digital Certificate Holder Application.

4.2.3. Time To Process Certificate Applications

Registration Authorities and Issuing CAs operating within the QuoVadis PKI are under no obligation to process Digital Certificate Applications other than within a commercially reasonable time.

4.3. Certificate Issuance

4.3.1. Certification Authority Actions During Certificate Issuance

Digital Certificate issuance is governed by and should comply with the practices described in and any requirements imposed by the QuoVadis CP/CPS.

4.3.1.1. QuoVadis Root Certification Authority

The Root Certification Authority Certificate has been self-generated and self-signed.

4.3.1.2. QuoVadis Issuing Certification Authority Certificates

Upon accepting the terms and conditions of the QuoVadis Issuing Certification Authority Agreement by the Issuing CA, successful completion of the Issuing Certification Authority application process as prescribed by QuoVadis, and final approval of the application by the QuoVadis Root Certification Authority, the QuoVadis Root Certification Authority issues the Issuing Certification Authority Digital Certificate to the relevant Issuing CA.

4.3.1.3. QuoVadis Registration Authority Appointment

Upon accepting the terms and conditions of the QuoVadis Registration Authority Agreement, successful completion of the Registration Authority application process and final approval of the application by the nominating Issuing CA, the Registration Authority becomes duly appointed, and appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

4.3.1.4. Registration Authority Officer's Certificate

As part of the application process, Registration Authorities are required to nominate one or more persons within their Organisation to take responsibility for the operation their

4.3.1.5. Certificate Holder Certificates

Upon the Applicant's acceptance of the terms and conditions of the Certificate Holder Agreement or other relevant agreement, the successful completion of the application process and final approval of the application by the Issuing CA, the Issuing CA issues the Digital Certificate to the Applicant or Device.

4.3.2. Notification To Applicant Certificate Holder By The Certification Authority Of Issuance Of Certificate

Issuing CAs and Registration Authorities within the QuoVadis PKI may choose to notify Applicants that their Digital Certificate has been issued.

4.4. Certificate Acceptance

Digital Certificate acceptance is governed by and should comply with the practices described in, and any requirements imposed by, this CP/CPS.

Until a Digital Certificate is accepted, it is not published in any Repository or otherwise made publicly available. By using a Digital Certificate, the Holder thereof certifies and agrees to the statements contained in the notice of approval. This CP/CPS sets out what constitutes acceptance of a Digital Certificate. An Applicant that accepts a Digital Certificate warrants to the relevant Issuing CA, and all Authorised Relying Parties who reasonably rely, that all information supplied in connection with the application process and all information included in the Digital Certificate issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a Digital Certificate or the reliance upon a Digital Certificate signifies acceptance by that person of the terms and conditions of this QuoVadis CP/CPS and Certificate Holder Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

By accepting a Digital Certificate issued by an Authorised Issuing CA operating within the QuoVadis PKI, the Certificate Holder expressly represents and warrants to QuoVadis and all Authorised Re

4.7.1. Circumstance For Certificate Re-Key
Digital Certificates may be renewed upon request.

4.7.2. Who May Request Re-Key
Certificate Holders and Nominating Registration Authorities may request Digital Certificate Re-Keys.

4.7.3. Processing Certificate Re-Key Request
Digital Certificate Re-Key requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS. In order to process a Re-Key request, the Digital Certificate Holder is required to confirm that:

- Details contained in the original Digital Certificate application have not changed.
- Authenticate their identity to the Registration Authority.

Using the Digital Certificate to be renewed, the Certificate Holder may digitally sign an electronic message to the Nominating Registration Authority requesting that the Digital Certificate be renewed and confirming that the original application details have not changed.

4.7.4. Notification Of New Certificate Issuance To Certificate Holder
Issuing CAs and Registration Authorities within the QuoVadis PKI shall notify Certificate Holders of Digital Certificate Issuance.

4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate
Downloading, installing or otherwise taking delivery of a re-keyed Digital Certificate constitutes acceptance of the Digital Certificate Re-Key within the QuoVadis PKI.

4.7.5.1. Publication Of The Re-Key Certificate By The Certification Authority
All Digital Certificate Re-Keys issued within the QuoVadis PKI are made available in public repositories except where Digital Certificate Holders have requested that their Digital Certificates not be published.

4.7.6. Notification Of Certificate Re-Key By The Certification Authority To Other Entities
Issuing CAs and Registration Authorities within the QuoVadis PKI may choose to notify other entities of Digital Certificate Re-Key.

4.8. Certificate Modification
The QuoVadis PKI does not support Digital Certificate Modification and the following do not apply to this CP/CPS:

- Circumstance for Digital Certificate modification.
- Who may request Digital Certificate modification.
- Processing Digital Certificate modification requests.
- Notification of new Digital Certificates issuance to subscriber.
- Conduct constituting acceptance of modified Digital Certificate.
- Publication of the modified Digital Certificate.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

4.9. Certificate Revocation And Suspension
4.9.1. Circumstances For Revocation
Digital certificates shall be revoked when any of the information on a Digital Certificate changes or becomes obsolete or when the private key associated with the Digital Certificate is compromised or suspected to be compromised. A Digital Certificate will be revoked in the following instances upon notification of:

- QuoVadis Certification Authority key compromise
- Digital Certificate Holder profile creation error
- Key Compromise including unauthorised access or suspected unauthorised access to private keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new certificate.

- The Digital Certificate Holder has failed to meet his, he

5.1.5. Fire Prevention And Protection

The QuoVadis secure operating area provides protection against fire according to DIN 4102 F90 with an automatic FM200 extinguishing system.

5.1.6. Media Storage

All magnetic media containing QuoVadis PKI information, including backup media, are stored in containers, cabinets or safes with fire and electromagnetic interference (EMI) protection capabilities and are located either within the QuoVadis service operations area or in a secure off-site storage area.

5.1.7. Waste Disposal

Paper documents and magnetic media containing trusted elements of QuoVadis or commercially sensitive or confidential information are securely disposed of by:

- in the case of magnetic media:
    -

5.4.3. Retention Period For Audit Log

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. Audit logs are stored until at least eleven (11) years after the QuoVadis Issuing Certification Authority ceases operation.

5.4.4. Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI.

Only Certification Authority Officers and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction.

All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures

Each Issuing CA performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing CA's premises and storage at a secure, off-site location.

Backup procedures apply to the QuoVadis PKI and the participants therein including the QuoVadis Root Certification Authority, Issuing CAs and Registration Authorities.

5.4.6. Audit Collection System

The security audit process of each Issuing CA runs independently of the Issuing CA software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7. Notification To Event-Causing Subject

Where an event is logged, no notice is required to be given to the Individual, Organisation, Device or Application that caused the event.

5.4.8. Vulnerability Assessment

Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the QuoVadis PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Issuing CA. Vulnerability assessment procedures intend to identify QuoVadis PKI threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders.

5.5. Records Archival

5.5.1. Types Of Records Archived

QuoVadis archives, and makes available upon authorised request, documentation related to and subject to the QuoVadis Document Access Policy. For each Digital Certificate, the records contain information related to creation, issuance, use, revocation, expiration, and renewal activities. These records will include all relevant evidence in the Issuing CA's possession including:

- Audit logs;
- Digital Certificate requests and all related actions;
- Contents of issued Digital Certificates;
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Digital Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- Digital Certificate Revocation Lists posted;
- Audit Opinions as discussed in this QuoVadis CP/CPS; and
- Name of the relevant QuoVadis Registration Authority.

5.5.2. Retention Period For Archive

QuoVadis Issuing Certification Authority archives will be retained and protected against modification or destruction for a period of eleven (11) years.

5.5.3. Protection Of Archive

Archives shall be retained and protected against modification or destruction. Only Certification Authority Officers, the QuoVadis Chief Security Officer, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.5.4. Archive Backup Procedures

QuoVadis maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

5.5.5. Requirements For Time-Stamping Of Records

- Entity private key compromise procedures.
- Entity Public Key Revocation procedures.
- Business continuity capabilities and procedures after a disaster.

5.8. Certification Authority And/Or Registration Authority Termination

When it is necessary to terminate an Issuing CA or Registration Authority service, the impact of the termination will be minimised as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements.

QuoVadis and each Issuing CA specify the procedures they will follow when terminating all or a portion of their

6.2.1. Cryptographic Module Standards And Controls

The generation and maintenance of the Root and Issuing CA private keys are facilitated through the use of an advanced cryptographic device known as a Hardware Security Module. The Hardware Security Module used by Issuing CAs in the QuoVadis PKI is designed to provide Federal Information Processing Standard-140 Level 4 and EAL 4 security standards in both the generation and the maintenance in all Root and Issuing CA private keys.

> For Qualified Certificates, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 standards.

6.2.2. Private Key (N Out Of M) Multi-Person Control

All CA Private Keys are accessed / activated through n-of-m multi-person control (e.g. a minimum threshold of splits of a private key decryption key must be used to decrypt or access the private CA signing key).

6.2.3. Private Key Escrow

Private Keys shall not be escrowed.

6.2.4. Private Key Backup

All Issuing CA Keys are held in secure cryptographic devices and are equally secured whenever stored outside the FIPS-boundary of the secure cryptographic device—never appearing in plaintext. Issuing CA Private Keys are stored in an encrypted state (using an encryption key to create a "cryptographic wrapper" around the key). Access is only by N-of-M control discussed above in Section 6.2.2. They are backed up under further encryption and maintained on-site and in secure off-site storage.

Certificate Holders may choose to backup their Private Keys by backing up their hard drive or the encrypted file containing their Keys.

6.2.5. Private Key Archive

Private Keys used for encryption shall not be archived, unless the Digital Certificate Holder or Registration Authority specifically cont4 >Autfeysss b(ys1)3(v0 Td[6.2.)7(2.)e.313 -1.207 Td(on-site an)-[(cate c 0.uTd[3(v)] Autat)3(e K0002echived, unle)]T

down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Certificate Holder's personal information.

6.4.3. Other Aspects Of Activation Data

Where a Personal Identification Code is used, the User is required to enter the Personal Identification Code and identification details such as their distinguished name before they are able to access and install their Keys and Digital Certificates.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Each Issuing CA must establish an approved System Security Policy that incorporates computer security technical requirements that are specific to that Issuing CA's operations.

The QuoVadis Issuing CA has established an approved System Security Policy that incorporates computer security technical requirements that are specific to QuoVadis and configured to allow the minimal amount of connectivity identified as being necessary to accomplish Certification Authority and Registration Authority functions.

Computer security technical requirements are achieved utilising a combination of hardened security modules and software, operating system security features, internal PKI and Certificate Authority Software and physical safeguards, including security Policies and Procedures that include but are not limited to:

- Access controls to Certificate Authority services and PKI roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and PKI roles, see Section 5.2
- Identification and Authentication of personnel that fulfil roles of responsibility in the QuoVadis PKI, see Section 5.3
- Use of cryptography for session communication and database security, mutually authenticated and encrypted SSL/TLS is used for all communications
- Archival of Certificate Authority history and audit data, see Sections 5.4 and 5.6
- Use of x.509 Digital Certificates for all administrators.

6.5.2. Computer Security Rating

QuoVadis has established an approved System Security Policy that incorporates computer security ratings that are specific to QuoVadis.

QuoVadis computer security ratings are achieved and maintained by real-time security monitoring and analysis, monthly security reviews by the QuoVadis Chief Security Officer and annual security reviews by external auditors.

6.6. Life Cycle Technical Controls

All hardware and software procured for operating an Issuing CA within the QuoVadis PKI must be purchased in a manner that will mitigate the risk that any particular component was tampered with, such as random selection of specific components. Equipment developed for use within the QuoVadis PKI shall be developed in a controlled

6.6.2. Security Management Controls

The QuoVadis Certificate Authority follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke and manage public key certificates, such as X.509 public key certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3. Life Cycle Security Controls

QuoVadis employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority systems. The Certificate Authority software, when first loaded will provide a method for QuoVadis to verify that the software on the system:

- Originated from the software developer
- Has not been modified prior to installation
- Is the version intended for use

The QuoVadis Chief Security Officer periodically verifies the integrity of the Certificate Authority software and monitors the configuration of the Certificate Authority systems.

6.7. Network Security Controls

All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

Any and all unused network ports and services are turned off to ensure that Issuing CA equipment is protected against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone, off-line configurations.

6.8. Time-Stamping

The QuoVadis Time-stamping Authority uses PKI and trusted time sources to provide reliable standards-based time-stamps. The QuoVadis Time-stamp Policy defines the operational and management practices of the QuoVadis Time-stamp Authority such that Participants and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

The QuoVadis Time-stamp Policy aims to deliver time-stamping services used in support of qualified electronic signatures, (i.e. in line with article 5.1 of the European

7.1.3. Algorithm Object Identifiers
No Stipulation.

7.1.4. Name Forms
See 3.1.1

7.1.5. Name Constraints
See 3.1.1

7.1.6. CP/CPS Object Identifier
The Object Identifiers (OIDs) assigned to this CP/CPS are 1.3.6.1.4.1.8024.0.1 and 1.3.6.1.4.1.8024.0.3.

7.1.7. Usage Of Policy Constraints Extension
No Stipulation.

7.1.8. Policy Qualifiers Syntax And Semantics
Digital Certificates issued within the QuoVadis PKI contain one of the Object Identifiers for this CP/CPS.

7.1.9. Processing Semantics For The Critical Certificate Policies Extension
No Stipulation.

7.2. Certificate Revocation List Profile
Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 3280.

7.2.1. Version Number
Issuing CAs within the QuoVadis PKI issue X.509 version 2 Certificate Revocation Lists.

7.2.2. Certificate Revocation List And Certificate Revocation List Entry Extensions
All User PKI software must correctly process all Certificate Revocation List extensions identified in the Digital Certificate and Certificate Revocation List profile.

7.3. Online Certificate Status Protocol Profile
Online Certificate Status Protocol is enabled for all Digital Certificates within the QuoVadis PKI.

7.3.1. Online Certificate Status Protocol Version Numbers
Version 1 of the Online Certificate Status Protocol, as defined by RFC2560, is supported within the QuoVadis PKI.

7.3.2. Online Certificate Status Protocol Extensions
No Stipulation.

7.4. Lightweight Directory Access Protocol Profile
QuoVadis will host a repository in the form of a Lightweight Directory Access Protocol directory for the purpose of (i) storing and making available all X.509 v. 3 Digital Certificates issued under the QuoVadis Certification Authority, (ii) facilitating public access to download these Digital Certificates for Digital Certificate Holder and relying party requirements, and (iii) receiving (from the QuoVadis Digital Certification Authority), storing and making publicly available, regularly updated Certificate Revocation List v. 2 information, for the purpose of Digital Certificate validation.

7.4.1. Lightweight Directory Access Protocol Version Numbers
LDAP V3 in accordance with RFC-3377

7.4.2. Lightweight Directory Access Protocol Extensions
No Stipulation.

7.5. Root And Issuing Certification Authority Profiles And Certificate Fields

7.5.1. Digital Certificate Fields

7.5.1.1. QuoVadis Root Certification Authority Certificate Profile

Field	QuoVadis Root Certificate Profile
Version	3
Serial Number	3ab6508b
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Validity	NotBefore: 3/19/2001 2:33 PM NotAfter: 3/17/2021 2:33 PM
Subject	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Subject Public Key Info.	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	Certificate Extensions: 6 1.3.6.1.5.5.7.1.1: Flags = 0, Length = 31 Authority Information Access [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://ocsp.quovadisoffshore.com 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None 2.5.29.32: Flags = 0, Length = 111 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certification practices, and the QuoVadis Certificate Policy. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: http://www.quovadis.bm 2.5.29.14: Flags = 0, Length = 16 Subject Key Identifier: 8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df 2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority OU=Root Certification Authority

Field	QuoVadis Issuing CA 2

7.5.1.3. QuoVadis Issuing CA 3 and QuoVadis Qualified Issuing CA 1: Swiss Jurisdiction – Qualified Certificates

Field	QuoVadis Issuing CA 3
Version	3
Serial Number	1109380779
Signature algorithm identifier	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer name	C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority
Period of validity	Not Before: Feb 15 21:46:22 2006 GMT Not After : Feb 15 21:46:22 2016 GMT
Subject name	C=CH O=QuoVadis Limited, Bermuda OU=Issuing Certification Authority CN=QuoVadis ICA 3
Subject's public-key information	Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	Certificate Extensions: 9 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None 1.3.6.1.5.5.7.1.1: Flags = 0, Length = 5c Authority Information Access [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://ocsp.quovadis.bm [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.quovadis.bm/trust/qvrca.crt 1.3.6.1.5.5.7.1.3: Flags = 1(Critical), Length = 18 QC Statements Qualified Digital Certificate id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) 2.5.29.32: Flags = 0, Length = 101 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the QuoVadis Certificate Policy & Certification Practice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: http://www.quovadis.bm 2.5.29.15: Flags = 1(Critical), Length = 4

Field	QuoVadis Qualified Issuing CA 1
	Path Length Constraint=None 1.3.6.1.5.5.7.1.1: Flags = 0, Length = 2e Authority Information Access [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48 .1) Alternative Name: URL=http://ocsp.quovadisglobal.com 1.3.6.1.5.5.7.1.3: Flags = 0, Length = 18 Unknown Extension type 0000 30 16 30 0a 06 08 2b 06 01 05 05 07 0b 02 30 08 0.0...+.....0. 0010 06 06 04 00 8e 46 01 01 .....F.. 2.5.29.32: Flags = 0, Length = e4 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the QuoVadis Certificate Policy/Certification Pr actice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/cps 2.5.29.15: Flags = 1(Critical), Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06) 2.5.29.18: Flags = 0, Length = 51 Issuer Alternative Name Directory Address:

Field	QuoVadis Qualified Issuing CA 1
	Cert Hash(sha1): 78 e2 dc c8 30 02 32 cb 15 79 0b 39 9b 23 3b ee 79 a5 c2 39

7.5.1.4. QuoVadis Root CA 3 Certificate Profile

Field	QuoVadis Root CA 3 Profile
Version	3
Serial Number	05c6
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Validity	NotBefore:11/24/2006 3:11:23 PM NotAfter: 11/24/2031 3:06:44 PM
Subject	CN= QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Subject Public Key Info.	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 4096 bits
Extensions	Certificate Extensions: 5 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None 2.5.29.32: Flags = 0, Length = d9 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 3 Certificate Policy / Certification Practice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/cps 2.5.29.15: Flags = 0, Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06) 2.5.29.14: Flags = 0, Length = 16 Subject Key Identifier f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 2.5.29.35: Flags = 0, Length = 67 Authority Key Identifier KeyID=f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Certificate Issuer: Directory Address: CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM Certificate SerialNumber=05 c6

Field	QuoVadis Root CA 3 Profile
	Signature Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash(sha1): 14 8d b3 54 ed 9b 2f 13 08 7c c3 8b 4b c1 5b 96 8a c5 53 78 Subject Key Id (precomputed): f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Cert Hash(md5): 31 85 3c 62 94 97 63 b9 aa fd 89 4e af 6f e0 cf Cert Hash(sha1): 1f 49 14 f7 d8 74 95 1d dd ae 02 c0 be fd 3a 2d 82 75 51 85

7.5.1.5. QuoVadis Root CA CRL Profile

Field	QuoVadis Root CA CRL	
Version	2	
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00	
Issuer	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM	CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Validity	ThisUpdate: Month/Day/Year NextUpdate: Month/Day/Year	
Extensions	CRL Extensions: 3 2.5.29.20: Flags = 0, Length = 3 CRL Number CRL Number=# 2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df or f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority or CN=QuoVadis Root CA 3 OU=Root Certification Authority O=QuoVadis Limited O=QuoVadis Limited C=BM C=BM Certificate SerialNumber=3a b6 50 8b or 05c6 2.5.29.28: Flags = 0, Length = 35 Issuing Distribution Point Distribution Point Name: Full Name: URL=http://www.quovadisoffshore.com/crl/qvrca.crl Only Contains User Certs=No Only Contains CA Certs=No Indirect CRL=No	
Signature Block	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00 CRL Hash(md5): ce ab 91 70 7f db 15 2d e4 6f 88 90 d1 3e 35 19 CRL Hash(sha1): ac 1e f1 0f 8b e0 8a e3 92 0d 4f 01 f7 11 0f 58 6d a4 27 68	

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency, Circumstance And Standards Of Assessment

8.1.1. QuoVadis Certification Authority

QuoVadis is subject to audits in respect of its various accreditations and certifications as follows:

Standards / Law	
Bermuda Accredited Certificate Service Provider	As defined in Bermuda's Electronic Transactions Act 1999, an Authorised Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.
Webtrust for Certification Authorities	The WebTrust Seal of assurance for Certification Authorities (CA) symbolises to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria.
SR 943.03 [ZertES]	Dated 21 December 2004 Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der (qualifizierten) elektronischen Signatur
SR 943.032 [VZertES]	Dated 6 December 2004 TAV Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur
SR 943.032.1 [TAV]	Dated 6 December 2004 (Ausgabe 1: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur („zur Anerkennung für qualifizierte elektronische Zertifikate“ nach Kapitel 2)
ESI (“Directive”)	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
ETSI [ESTI101456TS]	TS 101 456 v.1.4.1 January 2006 EU Standards Body Technical Specification - Policy Requirements for certification authorities issuing qualified certificates
ETSI [ESTI101862TS]	TS 101 862, v1.3.2 June 2004, Qualified Certificate Profile
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework corrigenda IETF RFC 3647 (including Erratum issued by IETF April 2004)

The results of these audits in the form of such publicly available audit reports as provided by the external auditors responsible for these audits will be published at www.quovadis.bm/audits. Compliance audits as carried out under these provisions may substitute for audits noted in this CP/CPS.

8.1.2. Issuing Certification Authorities

Issuing CAs (including QuoVadis) will undergo an audit in order to determine compliance with this QuoVadis CP/CPS at least annually. These audits shall include the review of all relevant documents maintained by the Issuing CA regarding operations within the QuoVadis PKI and under this QuoVadis CP/CPS, and other related operational policies and procedures.

8.1.3. Registration Authorities

Every Registration Authority within the QuoVadis PKI is subject to an annual compliance review performed by or on behalf of QuoVadis in order to determine compliance by those entities with their operational requirements within the QuoVadis PKI. The obligations of Issuing CAs and RegistratiQueir operational ir opere entTJ operational ir opere entT6 0.48 ref45.72 3

Ernst & Young. The accreditation audits for Swiss and European signature requirements have been performed by KPMG Klynveld Peat Marwick Goerdeler SA.

8.3. Assessor's Relationship To Assessed Entity

The auditor and the Issuing CA under audit, must not have any other relationship that would impair the auditor's independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

8.4. Topics Covered By Assessment

The topics covered by an audit of an Issuing CA will include but may not be limited to:

- Security Policy and Planning;
-

Certificate. Any decision regarding which of these actions to take will be based on QuoVadis' opinion of the severity and materiality of the irregularities.

8.6. Publication Of Audit Results

The audit opinion based on results of the audits will be generally available upon request. The results of the most recent audit of QuoVadis will be posted in the Repository located at www.quovadis.bm.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Issuing CAs and Registration Authorities within the QuoVadis PKI will make available all applicable fees upon request. Fees for Digital Certificate issuance vary widely based upon volumes and Digital Certificate types. Annual Fees for Qualified Digital Certificate Holder Certificates issued to individual public applicants are €100.00 (Euro)

9.1.1. Certificate Issuance Or Renewal Fees

Fees may be payable with respect to the issue or renewal of Digital Certificates--details of which are contained within the relevant contractual documentation governing the issue or renewal of such Digital Certificates.

9.1.2. Certificate Access Fees

Fees may be payable with respect to access to the QuoVadis X.500 Directory services for Digital Certificate downloading, details of which are contained in relevant contractual agreements.

9.1.3. Revocation Or Status Information Access Fees

Fees may be payable with respect to access to the QuoVadis X.500 Directory services for Certificate revocation or status information, details of which are contained in relevant contractual agreements.

9.1.4. Fees For Other Services

Fees may be levied in connection with the following:

- Digital Certificate revocation
- Private Encryption Key Archive and recovery;
- Digital Certificate status and Validation; and
- Policy access fees.

9.1.5. 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.

9.2. Financial Responsibilities

QuoVadis is responsible for maintaining its financial books and records in a commercially reasonable manner and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

9.2.1. Insurance Coverage

QuoVadis maintains in full force and effect a liability insurance policy. In accordance with the requirement of ZERT

9.2.3. Insurance Or Warranty Coverage For End-Entities

QuoVadis will give advice to and support the QuoVadis Certificate Holders and QuoVadis Relying Parties on questions relating to the different types of insurance available.

QuoVadis Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft,

determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the relevant CA and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the CA (e.g. those of the relevant EU Member).

9.4.7. Other Information Disclosure Circumstances

QuoVadis, Issuing CAs and Registration Authorities are under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order that complies with requirements of this CP/CPS.

9.5. Intellectual Property Rights

All Intellectual Property Rights including all copyright in all Digital Certificates and all documents (electronic or otherwise) belong to and will remain the property of QuoVadis.

Private Keys and Public Keys are the property of the applicable rightful Private Key holder. Digital Certificates issued and all Intellectual Property Rights including all copyright in all Digital Certificates and all documents (electronic or otherwise) belong to and will remain the property of QuoVadis.

9.8.3. Excluded Liability

QuoVadis shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorised disclosure or unauthorised use of the Digital Certificate or any password or activation data used to control access thereto;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or Organisation;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this QuoVadis CP/CPS and/or the relevant Certificate Holder Agreement or any applicable law or regulation;
- If the Private Key associated with the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised; or
- If the Digital Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation.
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that QuoVadis uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided QuoVadis uses commercially reasonable methods to protect against such disturbances;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of QuoVadis and/or its subcontractors or service providers; or
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which QuoVadis is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of QuoVadis.

9.8.3.1. Certificate Loss Limits

Without prejudice to any other provision of this Section 9, QuoVadis' liability for breach of its obligations pursuant to this QuoVadis CP/CPS shall, absent 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	$100,000.00
Device Certificate	$100,000.00

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.

9.8.4. Mitigation Of QuoVadis' Liability

QuoVadis has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by authorised personnel; or
- prohibit access to those resources by unauthorised individuals.

These measures include but are not limited to:

- identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
- performing regular system data backups;
- performing a backup of the current operating software and certain software configuration files;
- storing all backups in secure local and offsite storage;
- maintaining secure offsite storage of other material needed for disaster recovery;
- periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
- periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks; and
- periodically testing uninterrupted power supplies.

9.8.5. Claims Against QuoVadis Liability

9.8.5.1. Notification Period

QuoVadis shall have no obligation pursuant to any claim for breach of its obligations hereunder unless the claiming party gives notice to QuoVadis within ninety (90) days after the claiming party knew or ought reasonably to have known of a claim, and in no event more than three years after the expiration of the Digital Certificate held by the claiming party.

9.8.5.2. Mitigating Acts And Disclosure Of Supporting Information

As a precondition to QuoVadis' payment of any claim under the terms of this QuoVadis CP/CPS, a claiming party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such further agreements, instruments, and documents as QuoVadis may reasonably request in order to investigate a claim of loss made by a claiming party.

9.9. Indemnities

Indemnity provisions and obligations are contained within relevant contractual documentation.

9.10. Term And Termination

9.10.1. Term

This CP/CPS becomes effective upon publication in the QuoVadis Repository. Amendments to this CP/CPS become effective upon publication in the QuoVadis Repository.

9.10.2. Termination

This CP/CPS shall remain in force until it is amended or replaced by a new version.

9.10.3. Effect Of Termination And Survival

The provisions of this QuoVadis CP/CPS shall survive the termination or withdrawal of a Certificate Holder or Relying Party from the QuoVadis PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the QuoVadis PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11. Individual Notices And Communications With Participants

Electronic mail, postal mail, fax, and web pages will all be valid means for QuoVadis to provide any of the notices required by this QuoVadis CP/CPS, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid means of providing any notice required pursuant to this QuoVadis CP/CPS to QuoVadis unless specifically provided otherwise (for example in respect of revocation procedures).

9.12. Amendments

9.12.1. Procedure For Amendment

Amendments to this CP/CPS are made and approved by the QuoVadis Policy Management Authority. Amendments shall be in the form of an Amended CP/CPS or a replacement CP/CPS. Updated versions of this CP/CPS supersede and designated or conflicting provisions of the referenced version of the CP/CPS.

There are two possible types of policy change:

- the issue of a new CP/CPS ; or
-

If an existing CP/CPS requires re-issue, the change process employed is the same as for initial publication, as described above. If a policy change is determined to ha

For Qualified Certificates, in accordance with the Swiss Digital Signature law, all disputes shall be dealt with under Swiss Law.

9.15. Compliance With Applicable Law

This CP/CPS is subject to applicable law.

9.16. Miscellaneous Provisions

Not Applicable.

9.16.1. Entire Agreement

Not Applicable.

9.16.2. Assignment

Not Applicable.

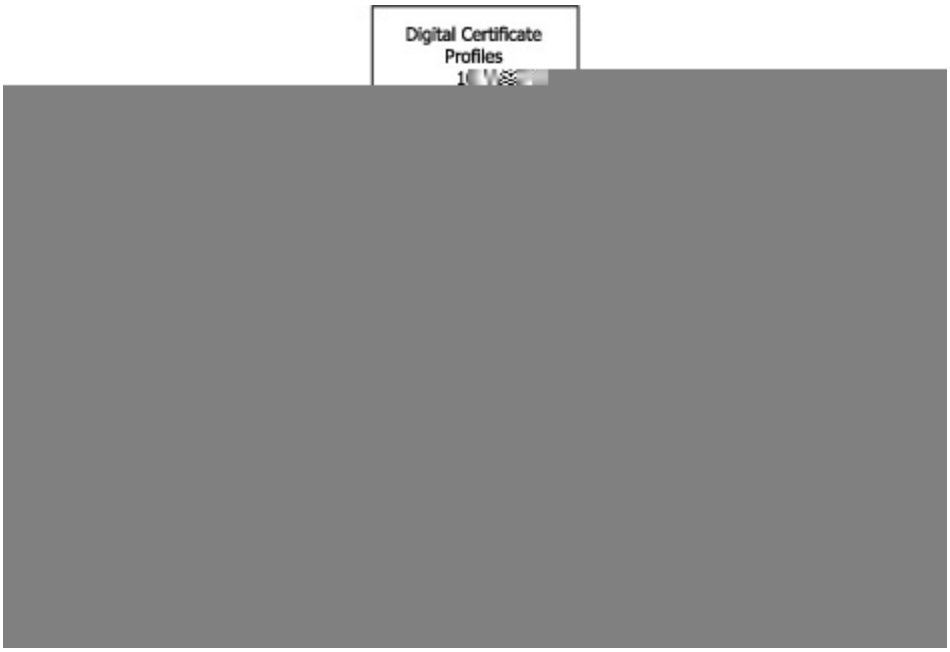
9.16.3. Severability

10. APPENDIX A
10.1. Digital Certificate Profiles

Within the QuoVadis PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. All Digital Certificate Profiles within the QuoVadis PKI are detailed below, (*See Diagram 3 and corresponding subsections below*).

The procedure for Digital Certificate Holder registration, Digital Certificate generation and distribution is described below for each type of Digital Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described in this CP/CPS may be drawn up under contract for individual customers.

Please note that where a Qualified Digital Certificate is issued within the meaning of European Union Directive 199/93/EC, the individual applying for the Qualified Digital Certificate must undergo a face-to-face identification and verification procedure.



The Certificate Profiles that follow indicate the fields which are VARIABLE on initial registration by the Certificate Holder (CH) and those which are FIXED by the Issuing CA either based on policy or by IETF Standard, applicable law or regulation.

10.1.1. 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 formation supplied i0 norrw/C20 ehta86.9e Cerhor

Key Usage	Data Encipherment (Optional)	CH Variable
Key Usage	Key Agreement (Optional)	CH Variable
Enhanced Key Usage	Client Authentication (Optional)	CH Variable
Enhanced Key Usage	Secure Email (Optional)	CH Variable
Enhanced Key Usage	Encrypting File System (Optional)	CH Variable
Enhanced Key Usage	Smart Card Logon (Optional)	CH Variable
Certificate Policies		

10.1.2 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.

DIGITAL CERTIFICATE GENERATION

All successful Standard Personal Digital Certificate requests will be processed by the QuoVadis Issuing Certification Authority. Each Standard Personal Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The QuoVadis Issuing Certification Authority will apply to the Digital Certificate request a:

- Unique serial number
- Operational Certification Authority's signature

DIGITAL CERTIFICATE DELIVERY

- Download over the Internet
- CD/Floppy Disk
- Smart Card or other secure hardware token

Certificate Pins are delivered in an out of band manner to the physical delivery method used for the Certificate.

FIELDS	CONTENT	DEMARCATION
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	Sha1RSA	Fixed
Issuer		
Common Name (CN)	Issuing Certification Authority Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Company Name	Fixed
Country (C)	Issuing Certification Authority Jurisdiction	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Standard Personal	Fixed OU) 806 a12 16 r176. 7TjR8 re

10.1.3 Qualified Certificate

Please note that where a Qualified Personal Digital Certificate is issued within the meaning of EU Directive 199/93/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

Date Of Birth	DD/MM/YYYY	CH Variable
Place of Birth	City	CH Variable
Gender	M/F	CH Variable
Title	Verified Legal Title	CH Variable
Country of Residence	ISO Country Code – Normally Resident	CH Variable
Country of Citizenship	ISO Country Code – Nationality	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / SyseResidencblee8 Td[sAU22[(Subject Public)7(Key Information)]TJEMC48	

10.1.4. 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 Stson:

Organisation (O)	QuoVadis Trust Services	Fixed
Country/Localitry	Variable Data	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	CH Variable
Key Usage	Digital Signature (Optional)	CH Variable
Key Usage	Non Repudiation (Optional)	CH Variable
Key Usage	Key Encipherment (Optional)	CH Variable
Key Usage	Data Encipherment (Optional)	CH Variable
Key Usage	Key Agreement (Optional)	CH Variable
Enhanced Key Usage	Client Authentication (Optional)	CH Variable
Enhanced Key Usage	Secure Email (Optional)	CH Variable
Enhanced Key Usage	Encrypting File System (Optional)	CH Variable
Enhanced Key Usage	Smart Card Logon (Optional)	CH Variable
Certificate Policies	htt<2t41 0 0 NfBT/P <</Gf5496 Ban1T/P <</Gf5496 BanTf0.0/MCID1r4ur73.88 9:e4 560.94 0	

Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)		

10.1.6. 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 i

Key Usage	Key Agreement (Optional)
Extended Key Usage	Server Authentication
Extended Key Usage	Client Authentication
Extended Key Usage	Code Signing
Extended Key Usage	IPSEC End Entity
Extended Key Usage	IPSEC Tunnel
Extended Key Usage	IPSEC User
Extended Key Usage	Timestamp
Extended Key Usage	OCSP Server
Extended Key Usage	Individual Code Signing
Extended Key Usage	Commercial Code Signing
Extended Key Usage	Trust Signature
Extended Key Usage	Microsoft Server Gated Cryptography
Extended Key Usage	Encrypted File System
Extended Key Usage	EFS Recovery
Extended Key Usage	Netscape Server Gated Cryptography
Extended Key Usage	Smartcard Logon
Certificate Policies	http://www.quovadis.bm/pn
Authority Information Access	https://www.ocsp.quovadisoffshore.com
Subject Alternative Name	Principle Name = Email Address
CRL Distribution	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl
Thumbprint Algorithm	Sha1
Thumbprint	System Generated

Policy Notice

11 APPENDIX B

11.1 Definitions and Acronyms

In this QuoVadis CP/CPS the following Key terms and Abbreviations shall have the following meaning in the operation of the QuoVadis PKI unless context otherwise requires:

"**Applicant**" means an Individual or Organisation that has submitted an application for the issue of a Digital Certificate.

"**Authorised Relying Party**" means an Individual or Organisation that has entered into a Relying Party Agreement authorizing that person or Organisation to exercise Reasonable Reliance on Digital Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

"**Authentication**" means the procedures and requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to provide against fraud, imitation and deception ("Authenticate" and "Authenticated" to be construed accordingly).

"**Certification**" means the process of creating a Digital Certificate for an entity and binding th

"**Digital Signature**" means data appended to, or a cryptographic transmission of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit.

"**Digital Transmission**" means the transmission of information in an electronic format.

"**Device**" means software, hardware or other electronic or automated means configured to act in a particular way without human intervention.

"**Device Certificate**" means a Digital Certificate issued to identify a Device.

"**Distinguished Name**

"**Public Key**" means a Key forming part of a Key Pair that can be made public.

"**Public Key Infrastructure**" **(PKI)** means a system for publishing the public key values used in public key cryptography. Also a system used in verifying, enrolling, and certifying users of a security application.

"**Qualified Certificate**" A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the 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.

"**QuoVadis**" means QuoVadis Limited, a Bermuda exempted company.

"**QuoVadis Issuing Certification Authority**" means QuoVadis in its capacity as an Issuing CA.

"**QuoVadis PKI**" means the infrastructure implemented and utilised by QuoVadis for the generation, distribution, management and archival of Keys, Digital Certificates and Certificate Revocation Lists and the Repository to which Digital Certificates and Certificate Revocation Lists are to be posted.

"**QuoVadis Root Certification Authority**" means QuoVadis in its capacity as a Root Certification Authority.

"**Registration Authority**" means a Registration Authority designated by an Issuing Certification Authority to operate within the QuoVadis PKI responsible for identification and authentication of Certificate Holders.

"**Registration Authority Agreement**" an agreement entered into between an Issuing CA and a Registration Authority pursuant to which that Registration Authority is to provide its services within the QuoVadis PKI.

"**Registration Authority Certificate**" means a digital i users of a securityS008]TJ/Tr Tdati9eistratite