CERTIFICATE POLICY - RCA

O.I.D: 1.3.6.1.4.1.8024.0.1.2000.1.2

Effective Date: September 6, 2005
Version: 2.09

Important Note About this Document

The information contained in this document is intended for personnel charged with the management and operation of the QV-PKI owned and operated by QuoVadis Limited.

You must not take any action or place any reliance on this document unless you are contractually entitled to do so. Contact:

Corporate Offices	**Mailing Address**
QuoVadis Limited	Suite 1640
3rd Floor	48 Par-La-Ville Road
Washington Mall,	Hamilton HM-11
7 Reid Street,	Bermuda
Hamilton HM-11,	
Bermuda	

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

This document is controlled and managed under the authority of the QuoVadis Policy Management Authority.

Version Control

	Date	Version	Description	Author
1	2001-08-01	2.02	Final	QuoVadis PMA
2	2002-02-25	2.05	Revised for CSP	QuoVadis PMA
3	2002-08-01	2.06	Revised for ARP	QuoVadis PMA
4	2003-08-05	2.07	Revised for WebTrust	QuoVadis PMA
5	2004-04-01	2.08	Revised for WebTrust	QuoVadis PMA
6	2005-09-06	2.09	Revised for WebTrust	QuoVadis PMA

Table of Contents

1. Introduction

1.1. Overview

QV1 Certificates;
QV2 Certificates;
QV3 Certificates;
QV4 Certificates; and
Device Certificates.

(QV1, QV2, QV3 and QV4 Certificates collectively hereinafter defined as “QV Type Certificates”)

The QV Type Certificates are differentiated on the basis of (i) the Identification and Authentication requirements applicable to each class of Certificate and (ii) QuoVadis’ limitation of liability as set out in Section 2.2. Details regarding certain characteristics (including the applicable Identification and Authentication requirements) of each class of QV Type Certificate is set out in Appendix B (QV Type Certificate Characteristics). The relationship between each of the QV Type Certificates and their respective Identification and Authentication requirements me8g0and ion0n398iemete7-fianpendix B

QuoVadis may provide Certificates pursuant to Certificate Policies that are separate and distinct in all respects from this QV-CP but that still operate and function within the QV-PKI. Any additional types of Certificates will be described pursuant to amendments to this QV-CP (that may be made by way of schedules hereto) or the adoption by QuoVadis of an additional Certificate Policy in each case following approval of the QV-PMA.

1.2.1.3. Certificate Characteristics

Certificate Characteristics for each of the QV Type Certificates are attached as Appendix B to this

1.4.1. Participants

This policy is applicable to QuoVadis in its capacity as both the QV-RCA and QV-CA, QV Issuing CAs, QV-RAs, QV-RAOs, QV Corporate RAs, Sponsoring Organisations, Subscribers and Authorised Relying Parties.

1.4.2. QuoVadis Root CA

The QuoVadis Public Key Infrastructure contains three Root CA's, each with a distinct name. The QuoVadis Root CA named "QV-RCA" issues QV Issuing CA Certificates in accordance with this QV-CP and related operational documents.

1.4.3. QV Issuing CAs

QV Issuing CAs are Organisations authorised by QuoVadis to participate within the QV-PKI and to create, issue, sign, revoke, and otherwise manage Certificates in accordance with their respective QV Issuing CA Agreement and this QV-CP. Generally, QV Issuing CAs will be authorised to issue and manage all types of Certificate supported by this QV-CP. An Organisation wishing to participate in the QV-PKI, in the capacity as a QV Issuing CA, must supply to QuoVadis' satisfaction evidence of that Organisation's ability to operate in accordance with the performance standards; and other obligations that QuoVadis, in its sole discretion, requires of its QV Issuing CAs. Organisations wishing to act as QV Issuing CAs will be required to enter into a QV Issuing CA Agreement and to act in accordance with QV Issuing CA operational policies, procedures and related documentation. Without limitation to the generality of the foregoing, QV Issuing CAs are required to act in accordance with and to be bound by the terms of this QV-CP. A QV Issuing CA may, but shall not be obliged to, detail its specific practices and other requirements in a Certification Practice Statement adopted by it following approval by the QV-PMA. QuoVadis, in addition to acting as the QV-RCA, also acts as a QV Issuing CA in accordance with this QV-CP. Notwithstanding that a QV Issuing CA may delegate certain functions to a QV-RA, the QV Issuing CA shall retain all responsibility for the management of any Certificates issued by it.

1.4.4. Registration Authorities

QV Issuing CAs may, subject to the approval of QuoVadis, designate specific QV-RAs to perform the Identification and Authentication and Certificate request and revocation functions defined by this QV-CP and related documents. All QV-RAs are required to fulfil their functions and obligations in accordance with this QV-CP and an RA Agreement to be entered into between the QV-RA and the relevant QV Issuing CA.

1.4.5. QV Corporate Registration Authorities

Organisations may become QV Corporate RAs (QV-CRA) within the QV-PKI. QV-CRAs may only request the issue of QV 4 Certificates to their employees and may request the issue of QV2 Certificates and QV3 Certificates to Affiliated Persons. QV-CRAs are required to perform Identification and Authentication requirements for their employees and Affiliated Persons and to fulfil their functions pursuant to a QV Corporate RA Agreement with QuoVadis and to comply with documentation directly to QV Issuing CAs. Sponsoring Organisations do not have the ability to permit the provision of Certificates directly within the QV-PKI.

1.4.7. Subscribers

Subscribers are Individuals or Organisations to whom Certificates are issued. Subscribers may be natural persons, commercial or non-profit making organisations, or national or state government departments, agencies, or authorities.

Subscribers are bound by the conditions of use of Certificates as contained in a User Agreement or otherwise applicable to them and their participation within the QV-PKI.

1.4.8. Authorised Relying Parties

Authorised Relying Parties are Individuals or Organisations who are authorised by contract to exercise Reasonable Reliance on Certificates in accordance with the terms and conditions of this QV-CP and a Relying Party Agreement. All User

2.1.2. QV Issuing CA Obligations

QV Issuing CAs are responsible for the management of all Certificates issued by them. The management of Certificates includes all aspects associated with an application for the issue of a Certificate, including any required Identification and Authentication process, and the issue, revocation, and renewal of Certificates. QV Issuing CAs, if authorised to do so by QuoVadis, may rely on (i) third party QV-RAs (ii) QV-CRAs and (iii) Sponsoring Organisations in the performance of Identification and Authentication requirements. In circumstances where a QV Issuing CA has relied on either a third party QV-RA, QV-CRA, or Sponsoring Organisation, that QV-RA, QV-CRA, or Sponsoring Organisation will bear sole responsibility and liability for the Identification and Authentication of Applicants that it processed. In circumstances where Identification and Authentication has been conducted by a QV-RA, QV-CRA, or Sponsoring Organisation, a QV Issuing CA is not obliged to check or verify that the relevant Identification and Authentication procedures were duly complied with and bears no responsibility for and shall not be liable for that Identification and Authentication. Notwithstanding the foregoing, any QV Issuing CA that relies upon the services of a QV-RA, QV-CRA, or Sponsoring Organisation is required to conduct regular compliance audits of that QV-RA, QV-CRA or Sponsoring Organisation with respect to their respective contractual commitments (that include the performance of Identification and Authentication requirements) and this QV-CP. QV Issuing CAs are required to ensure that all aspects of the services they offer and perform within the QV-PKI are in compliance at all times with this QV-CP. Without limitation to the generality of the foregoing, QV Issuing CAs are required to adhere to the following requirements:

2.1.2.1. Certificate Issuance and Revocation

Each QV Issuing CA is required to maintain and make available a Repository together with a Certificate Revocation List (CRL). The information contained in both the Repository and the CRL maintained by QV Issuing CAs is required to be made available to Authorised Relying Parties in accordance with this QV-CP.

2.1.2.2. Warranties

Each QV Issuing CA is required to ensure that warranties, if any, provided by QuoVadis in connection with this QV-CP to Subscribers and Authorised Relying Parties are incorporated, by reference or otherwise, in the relevant User Agreement or applicable terms and conditions. Warranties, if any, provided by QuoVadis to Subscribers and/or Authorised Relying Parties shall be set out in a warranty protection plan duly approved by the PMA and adopted by QuoVadis.

2.1.2.3. Subscriber Obligations

QV Issuing CAs are obligated to ensure that Subscribers are bound by and comply with the provisions of this QV-CP either through the entry into of a User Agreement or otherwise through the acceptance of contractually binding terms and conditions.

2.1.2.4. Protection of Private Keys

Each QV Issuing CA must protect its Private Keys in accordance with the provisions of this QV-CP.

2.1.2.5. Use of Private Keys

QV Issuing CAs are required to ensure that their Private Keys are used only in connection with the signature of Certificates and CRLs.

2.1.2.6. QV-RAs and QV-CRAs

QV Issuing CAs are required to ensure that their designated QV-RAs, whether in-sourced or outsourced; and their QV-CRAs operate in compliance with this QV-CP and other related documents.

2.1.4.3. Revocation

Process Certificate Revocation requests in accordance with this QV-CP, applicable QV-CRA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the QV-CRA shall request the revocation of any QV4 Certificate that it has approved for issuance where the Individual identified by that Certificate (i) is no longer employed by the QV-CRA; (ii) is no longer authorised to act on behalf of the QV-CRA through the use of the QV4 Certificate; or (iii) for any other reason, in the sole discretion of QuoVadis or the QV-CRA, becomes unsuitable or unauthorised by the QV-CRA to hold a QV4 Certificate.

2.1.4.4. Compliance

Comply with the provisions of its QV-CRA Agreement and the provisions of this QV-CP including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements.

2.1.5. Sponsoring Organisation Obligations

Sponsoring Organisations are required to act in accordance with their relevant Sponsoring Organisation Agreement. Without limitation to the generality of the foregoing, each Sponsoring Organisation shall:

2.1.5.1. Certificate Applications

In connection with any application for the issue of Certificates, ensure that it has conducted the appropriate Identification and Authentication requirements for the Certificate type applied for and provide sufficient information and documentation in support of that application to the relevant QV Issuing CA.

2.1.5.2. Records

Maintain complete and up to date records related to its application for the issuance of Certificates together with all supporting documentation.

2.1.5.3. Revocation

Act in connection with Certificate Revocation requests in accordance with this QV-CP and applicable Sponsoring Organisation Agreement. Without limitation to the generality of the foregoing, the Sponsoring Organisation shall request the revocation of any QV4 Certificate that it has approved for issuance where the Individual identified by that Certificate (i) is no longer employed by the Sponsoring Organisation; or (ii) for any other reason becomes unsuitable or unauthorised, in the sole discretion of QuoVadis or the Sponsoring Organisation, by the Sponsoring Organisation to hold a QV4 Certificate.

2.1.5.4. Compliance

Comply with the provisions of its Sponsoring Organisation Agreement and the provisions of this QV-CP including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements.

2.1.6. Subscriber Obligations

Subscribers are required to act in accordance with their relevant User Agreement or other terms and conditions applicable to the use of the QV-PKI and their Certificate. Without limitation to the generality of the foregoing, each Subscriber shall be obliged to:

2.1.6.1. Information

Provide complete, full, and accurate information in connection with its application for the issue of a Certificate.

2.1.6.2. Identification and Authentication

Comply fully with any and all information and

Loss Limits/Reliance Limits

Loss Limits	
Certificate	**Maximum per Certificate**
QV1 Certificate	$1,000
QV2 Certificate	$50,000
QV3 Certificate	$10,000
QV4 Certificate	$100,000
Device Certificate	$100,000

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 Certificate to the intent that the loss limits reflect QuoVadis' total potential cumulative liability per Certificate per year (irrespective of the number of claims per Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Certificate in any one year of that Certificate's life cycle.

2.2.2.2. Excluded Liability

Notwithstanding any other provisions of this Section 2, QuoVadis shall bear no liability for loss involving or arising from any one (or more) of the following circumstances or causes:

a) Computer hardware or software, or mathematical algorithms, are developed that tend to maB4u3e507 Tw79.00 Certif

the professional services of an internationally recognized accounting/auditing firm to provide financial services, including periodic audits.

2.3.4. Demonstration of Financial Responsibility

QV Providers are required to demonstrate that they have the financial resources necessary to discharge their obligations as QV Providers. Without limitation to the generality of the foregoing, QuoVadis and each QV Issuing CA, QV-RA, and QV-CRA shall maintain appropriate insurances necessary to provide for their respective liabilities as participants within the QV-PKI. The failure of a QV Provider to maintain insurances may be the basis for the revocation of their respective Certificates.

2.4. Interpretation and Enforcement

2.4.1. Governing Law

This QV-CP is governed by the laws of Bermuda without reference to conflicts of law principles.

2.4.2. Severability, Notice

Any provision of this QV-CP that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this QV-CP or affecting the validity or enforceability of such remaining provisions.

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

2.4.3. Survival

The provisions of this QV-CP shall survive the termination or withdrawal of a User from the QV-PKI with respect to all actions based upon the use of or reliance upon a Certificate or other participation within the QV-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.

2.4.4. Waiver

The failure or delay of QuoVadis to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise have been amended or supplemented. In the event of a conflict, the provisions of this QV-CP will control.

(ii) The party desiring the arbitration shall give written notice to the other parties, naming an arbitrator of its choice. Within ten (10) days of such notice, the other parties shall designate a single arbitrator each. Within ten (10) days of the designation of the arbitrators as aforesaid, the arbitrators shall jointly designate a third arbitrator in the event that there are only two parties to the proceedings. In the event that there are more than two arbitrators appointed by the parties, then the arbitrators shall not designate an additional arbitrator. The parties shall thereafter submit the dispute to the designated arbitrators for resolution.

(iii) In the event the above-mentioned does not take place within the specified time then the arbitration will be conducted before a panel of three arbitrators, regardless of the size of the dispute or the number of parties, to be selected as provided in the UNCITRAL Rules. Any issue concerning the extent to which any dispute is subject to arbitration, or concerning the applicability, interpretation, or enforceability of these procedures, including any contention that all or part of these procedures are invalid or unenforceable, shall be governed by the relevant Bermuda laws and resolved by the arbitrators. No potential arbitrator may serve on the panel unless he or she has agreed in writing to abide and be bound by these procedures.

(iv) The arbitrators may not award non-monetary

2.5. Publication and Repository

2.5.1. Publication of QV Issuing CA Information

The QV-RCA and each QV Issuing CA shall each maintain and publish in a Repository copies of all Certificates issued by the QV Issuing CA's and CRLs advising of revocation of any such Certificates. QuoVadis publishes this QV-CP in the web based PKI repository located at www.quovadis.bm.

2.5.2. Frequency of Publication

Certificates are published immediately upon issuance. CRL publication will be in accordance with section 4.4.8. Policy publication will be in accordance with Section 8.

2.5.3. Access Control

The documents specified in Section 2.6.1 are to be available to Relying Parties twenty-four hours per day, seven days per week, except for reasonable maintenance requirements, where access is deemed necessary.

2.6. Compliance Audit

2.6.1. QV Issuing CAs

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

2.6.1.1. Identity/Qualifications of Auditor

The audit services described in Section 2.7.1 are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms provided they are qualified to perform and experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies.

2.6.1.2. Auditor's Relationship to Audited Party

The auditor and the QV Issuing CA under audit, must not have any other relationship that would impair its 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.

2.6.1.3. Topics Covered by Audit

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

- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;
- Contracts; and
- Privacy Considerations.

2.6.1.4. Actions Taken as a Result of Deficiency

If irregularities are found, the QV Issuing CA must submit a report to QuoVadis as to any action the QV Issuing CA will take in response to the irregularity. Where the QV Issuing CA fails to take appropriate action in response to the irregularity, QuoVadis may (i) indicate the irregularities, but allow the QV Issuing CA to continue operations for a limited period of time; (ii) allow the QV Issuing CA to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation of that QV Issuing CAs Certificate; (iii) limit the class of any Certificates issued by the QV Issuing CA; or (iv) revoke the QV Issuing CA's Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary cessation of QV Issuing CA services, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of any remedy.

In circumstances where any irregularities are found with respect to QuoVadis, in its capacity as a QV Issuing CA, the principles enunciated above will be followed by QuoVadis.

2.6.1.5. Communication of Results

and Sponsoring Organisations may perform the Identification and Authentication required in connection with the issue of QV3 and QV4 Certificates to their Affiliated Persons.

3.1.2. Types of Names

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

Identify an Individual or Organisation and to demonstrate that the Individual or Organisation exists and is who it claims to be.

3.1.7.1. Organisations

The Identity of an Organisation is required to be Authenticated with respect to each 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 QV-CRA or Sponsoring Organisation with respect to the issuance of QV3 and QV4 Certificates to its employees and/or QV3 and QV4 Certificates to its Affiliated Persons is required to be Authenticated.

In order to Authenticate the Ident

which shall reliably establish the Identity of the Affiliated Person. Such records shall establish, at a minimum, that the QV-RA, QV-CRA or Sponsoring Organisation has previously had occasion to Authenticate the Identity of the Affiliated Person (for example, in the context of fulfilling a Know-Your-Customer requirement), and the nature of the information upon which the QV-RA, QV-CRA, or Sponsoring Organisation relied upon for this purpose.

Where a QV-RA, QV-CRA or Sponsoring Organisation has a pre-existing shared secret with an Affiliated Person (such as UserID and password), and the QV-RA, QV-CRA or Sponsoring Organisation has previously Authenticated the Identity of the Affiliated Person in accordance with the requirements set forth above, the QV-RA, QV-CRA or Sponsoring Organisation may request the issue a QV3 Certificate to the Affiliated Person on the basis of that shared secret, provided that the QV-RA, QV-CRA or Sponsoring Organisation has no reason to believe that anyone other than the Affiliated Person has knowledge of the shared secret.

A QV-RA, QV-CRA or Sponsoring Organisation approving the issuance of a QV2 Certificate to an Affiliated Person may Authenticate the Identity of the Affiliated Person by reference to business records maintained by the QV-RA or Sponsoring Organisation, which shall reliably establish the Identity of the Affiliated Person but that fail to meet that QV-RA's, CRA's, or Sponsoring Organisation's Know-Your-Customer requirements. In such circumstances a letter confirming certain issues as to Identity and affiliation of the Applicant will be required from the Applicant's employer.

3.1.7.4. Individuals

With the exception of QV1 Certificates, that are issued on the basis of Applicant self-certification only, the Authentication of an Applicant's Identity must be based upon at least (i) one form of government-issued photographic identification; and (ii) 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 Certificate application. With respect to each form of government-issued photographic identification, that identification should be independently verified to ensure that it corresponds to a 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).

Registration information may be received from an Applicant either (i) in person; or (ii) by mail or electronic methods. Where registration information

3.3. Rekey After Revocation or Expiration

QV Issuing CAs in the QV-PKI may not re-key revoked Certificates. All Certificates must be renewed by following the initial application process.

4. Operational Requirements

4.1. Certificate Application

4.1.1. Request

An application in a form prescribed by the QV Issuing CA must be completed by Applicants, which includes all registration information as described by this QV-CP (including, without limitation, that information set out in Appendix B) and the relevant User Agreement or other terms and conditions upon which the Certificate is to be issued. All applications are subject to review, approval, and acceptance by the QV Issuing CA in its discretion.

Certain information concerning applications for Certificates is set out in this QV-CP. However, the issue of Certificates by QV Issuing CAs will be pursuant to forms and documentation required by that QV Issuing CA. Notwithstanding the foregoing, the following steps are required in any application for a Certificate: (i) Identity of the Holder or Device is to be established in accordance with Section 3 and Appendix B, (ii) a Key Pair for the Certificate is to be generated in a secure fashion, (iii) the binding of the Key Pair to the Certificate shall occur as set forth in Section 6.1, and (iv) the QV Issuing CA shall enter into contractual relations for the use of that Certificate and the QV-PKI. Individuals and Organisations may generate a Certificate application.

4.1.2. Process

Each QV Issuing CA will adopt their own application forms and procedures that Applicants will be required to satisfy. Each Holder of a Certificate is required 1 User Aficon f y6(wilea.33 1epns foration)53.1 he0.0098rw

(v) The QV Issuing CA is requested to revoke a Certificate by a QV-RA, QV-CRA, or Sponsoring Organisation (in connection with Certificates approved for issuance by them); or

(vi) The QV Issuing CA determines that a Certificate was not issued correctly in accordance with this QV-CP.

In the event that the QV issuing CA determines that the Certificates or the QV-PKI have been, or could become compromised, and that revocation of Certificates is in the interests of the QV-Providers, following remedial action, QV will reissue certificates to Subscribers at no charge, unless the actions of the Subscriber were in breach of the QV-CP or other contractual documents.

4.4.2. Who Can Request Revocation

The following entities may request revocation of a Certificate issued by a QV Issuing CA:

(i) a Holder via the Issuing CA and QV-RA, QV-CRA or Sponsoring Organisation that caused the Certificate to be issued;

(ii) an authorised representative of the QV-CRA or Sponsoring Organisation with which the Certificate is affiliated (if any),

(iii) the QV Issuing CA for that Certificate;

(iv) the QV-RA (if any) that approved the issuance of that Certificate; or

(v) QuoVadis.

4.4.3. Procedure for Revocation Requests

A revocation request should be promptly directly communicated to the QV Issuing CA, and the QV-RA, QV-CRA, or Sponsoring Organisation that approved or acted in connection with the issue thereof. A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Holder requesting revocation (or the Organisation, where applicable). Alternatively, the Holder (or Organisation, where applicable) may request revocation by contacting the QV Issuing CA and providing adequate proof of identification in accordance with

Failure to do so negates the ability of the Authorised Relying Party to claim that it acted on the Certificate with Reasonable Reliance.

4.4.8. On-Line Revocation/Status Checking Availability

When a QV Issuing CA provides on-line Certificate status database as a method of verifying the validity and status of Certificates, the Authorised Relying Party must validate the Certificate in accordance with that method.

4.4.9. On-Line Validation Requirements

Authorised Relying Parties who rely on an online Certificate status database must (i) validate a Certificate with such database before relying on that Certificate, and (ii) log the validation request.

Backup procedures apply to the QV-PKI and the participants therein including the QV-RCA, QV Issuing CAs, QV-RAs, and QV-CRAs.

4.5.6. Audit Collection System

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

4.5.7. Vulnerability Assessments

Both baseline and ongoing threat and risk vulnerability assessments will be carried out on all parts of the QV-PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each QV Issuing CA. Vulnerability assessment procedures intend to identify QV-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.

4.6. Records Archival

4.6.1. Types of Events Recorded

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

(i) Audit logs;
(ii) Certificate requests and all related actions;
(iii) Contents of issued Certificates;
(iv) Evidence of Certificate acceptance and signed (electronically or otherwise) User Agreements;
(v) Certificate renewal requests and all related actions;
(vi) Revocation requests and all related actions;
(vii) CRLs posted;
(viii) Audit Opinions as discussed in this QV-CP; and
(ix) Name of the relevant QV-RA, QV-CRA, or Sponsoring Organisation.

4.6.2. Retention Period for Archive

QV Issuing CA archives will be retained and protected against modification or destruction for a period of 7 (seven) years.

4.6.3. Protection of Archive

Only CAOs 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 recognized representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval. Requests for access to archived information should be sent electronically to QuoVadis.

4.6.4. Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

4.6.5. Requirements for Timestamping Records

QuoVadis supports time stamping of all of its records.

5.2. Procedural Controls

5.2.1. Trusted Roles

To ensure that one person acting alone cannot circumvent safeguards, responsibilities for the QV Issuing CA are distributed among multiple roles and individuals. A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill trusted roles must be careful and above reproach. The functions performed in trusted roles form the basis of trust in the QV-PKI.

5.2.2. Number of Individuals Required per Role

Procedures must be in place to ensure that one individual acting alone may not perform any of the trusted roles except verifying and reviewing audit logs. QV Issuing CAs will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. QV Issuing CAs must ensure that no single Individual may gain access to a User's Private Key if stored by the QV Issuing CA. At a minimum, procedural or operational mechanisms must be in place for QV Issuing CA Key recovery in disaster recovery situations. To best ensure the integrity of the QV Issuing CA equipment and operation, QV Issuing CAs will use commercially reasonable efforts to identify a separate individual for each trusted role.

5.2.3. Identification and Authentication for Each Role

Each individual performing any of the trusted roles shall use a QuoVadis issued Certificate stored on an approved cryptographic smart card to identify themselves to the Certificate server and Repository.

5.3. Personnel Controls

For purposes of mitigating the risk that one Individual acting alone could compromise the integrity of the QV-PKI or any Certificate issued therein, QuoVadis shall perform relevant background checks of individuals and define tasks that the Individuals will be responsible to perform. QuoVadis shall determine the nature and extent of any background checks, in its sole discretion. The foregoing fully stipulates QuoVadis' obligations with respect to personnel controls and QuoVadis shall have no other duty or responsibility with respect to the foregoing. Without limitation, QuoVadis shall not be liable for employee conduct that is outside of their duties and for which QuoVadis has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

All Key Pairs will be generated in a manner that QuoVadis, in its sole discretion, deems to be secure.

6.1.2. Private Key Delivery

In most cases, a Private Key will be generated and remain within the Cryptomodule. If the owner of the Cryptomodule generates the Key, then there is no need to deliver the Private Key. If a Key is not generated by the intended Key holder, then the person generating the Key in the Cryptomodule (e.g., smart card) must securely deliver the Cryptomodule to the intended Key holder. Accountability for the location and state of the Cryptomodule must be maintained until delivery and possession occurs. The recipient will acknowledge receipt of the Cryptomodule to the QV Issuing CA, QV-RA, or QV-CRA. If the recipient generates the Key, and the Key will be stored by and used by the application that generated it, or on a Token in the possession of the

6.2.4. Private Key Backup

The Private Keys may be backed up during the regular backup cycle. They will be encrypted on the backup, so they are still secure. Users may backup their own Private Key. The same level of protection shall be given to the back up copy as to the primary copy.

7.2.2. CRL and CRL Entry Extension

All User QV-PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The applicable CPS or other public

APPENDIX A

Definitions and Interpretation

In this QV-CP the following expressions shall have the following meanings unless the context otherwise requires:

“**Affiliated Person**” means an Individual known to a QV-RA, QV-CRA or Sponsoring Organisation as (i) a customer of the QV-RA, QV-CRA or Sponsoring Organisation to whom the QV-RA, QV-CRA or Sponsoring Organisation provides goods or services, and who the QV-RA, QV-CRA or Sponsoring Organisation is reliably able to identify through business records maintained by the QV-RA, QV-CRA or Sponsoring Organisation; or (ii) an agent or employee of an Organisation with which the QV-RA, QV-CRA or Sponsoring Organisation maintains a regular business relationship, and who the QV-RA, QV-CRA or Sponsoring Organisation is reliably able to identify through business records maintained by the QV-RA, QV-CRA or Sponsoring Organisation;
“

"**Device**" means software, hardware or other electronic or automated means configured to act in a particular way without human intervention;
"**Device Certificate**" means a Certificate issued to identify a Device;
"**Distinguished Name**" or "**DN**" means the unique identifier for the Holder of a Certificate;
"**Holder**" means an Individual or Organisation that is (i) named in a Certificate or responsible for the Device named in a Certificate and (ii) holds a Private Key corresponding to the Public Key listed in that Certificate;
"**Identify**

APPENDIX B

CERTIFICATE CHARACTERISTICS

REQUIRED INFORMATION FOR APPLICATIONS SUBMITTED TO A QV-RA

QV1 Certificate	QV2 Certificate	QV3 Certificate	QV4 Certificate
Full name of Applicant:	Full name of Applicant:	Full name of Applicant:	Full name of Applicant:
Street Address: (Residential)	Street Address: (Residential)	Street Address: (Residential)	Street Address: (Residential)
City	City	City	City
State/Province	State/Province	State/Province	State/Province
Country	Country	Country	Country
ZIP/Postal Code	ZIP/Postal Code	ZIP/Postal Code	ZIP/Postal Code
E-mail address:	E-mail address:	E-mail address:	E-mail address:
Home Telephone Number:	Home Telephone Number:	Home Telephone Number:	Home Telephone Number:
Work Telephone Number (if applicable):	Work Telephone Number (if applicable):	Work Telephone Number (if applicable):	Work Telephone Number (if applicable):
Nationality	Nationality	Nationality	Nationality
Passport/Government Identification Number:	Passport/Government Identification Number:	Passport/Government Identification Number:	Passport/Government Identification Number:

OPTIONAL INFORMATION

Not Applicable	Organisational Name	Organisational Name	Organisational Name

IDENTIFICATION

QV1 Certificate	QV2 Certificate	QV3 Certificate	QV4 Certificate
None	Copy of Passport or other Government issued Identification document	N/A –Organisation requesting Certificate attests to veracity of information contained therein	N/A –Organisation requesting Certificate attests to veracity of information contained therein
None	Copy of Utility bill or Bank Statement showing the name and address as completed on the Application Form		

OPTIONAL INFORMATION

Not Applicable	A letter on headed paper addressed to QuoVadis Limited confirming the applicant's affiliation with that Organisation together with a statement to the effect that the Organisation has no objection to the inclusion of its name in the applicant's Certificate.	A letter on headed paper addressed to QuoVadis Limited confirming the applicant's affiliation with that Organisation together with a statement to the effect that the Organisation has no objection to the inclusion of its name in the applicant's Certificate.	A letter on headed paper addressed to QuoVadis Limited confirming the applicant's affiliation with that Organisation together with a statement to the effect that the Organisation has no objection to the inclusion of its name in the applicant's Certificate.

AUTHENTICATION

QV1 Certificate	QV2 Certificate	QV3 Certificate	QV4 Certificate
N/A	Documentary Check	Documentary Check	Documentary Check
N/A	Documentation certified as true by either: □a financial institution that is subject to Know Your Customer requirements, or □an authorised notary or □a QV-RA, or in person appearance before a QV-RA and presentation of original documentation.	Organisation requesting Certificate attests to veracity of information contained therein.	Organisation requesting Certificate attests to veracity of information contained therein.

CERTIFICATE CHARACTERISTICS

REQUIRED INFORMATION for APPLICATIONS SUBMITTED BY A SPONSORING ORGANISATION OR CORPORATE RA

QV 1 Certificate	**QV2 Certificate**	**QV3 Certificate (for Employees, Trading Partners, Clients or Affiliates only)**	**QV4 Certificate (for Employees, Trading Partners, Clients or Affiliates only)**
Not Applicable	Not Applicable	Organisation Name of Trading Partner, Client, or Affiliate (if desired)	Organisation Name of Sponsoring Organisation or Corporate RA
Not Applicable	Not Applicable	Organisational Unit (if desired)	Organisational Unit (if desired)
[redacted]able	Not Applicable	Full name of Applicant:	Full name of Applicant: