CERTIFICATE POLICY - RCA

O.I.D: 1.3.6.1.4.1.8024.0.1.2000.1.2

Effective Date: March 1, 2004
Version: 2.08

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

Mailing Address
Suite 1640
48 Par-La-Ville Road
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

Table of Contents

1. Introduction

1.1. Overview

This QuoVadis Certificate Policy (QV-CP) sets out the policies and requirements that are followed in the generation, issuance, use, and management of Certificates supported within the QuoVadis Public Key Infrastructure (QV-PKI) and the roles, responsibilities, and relationships of persons authorized to participate within the QV-PKI. This QV-CP has been adopted and approved by the QuoVadis Policy Management Authority (QV-PMA) and undergoes a regular review process as prescribed by the QV-PMA. Revisions of this QV-CP are identified, communicated, and adopted and amended, from time to time by the QV-PMA.

Matters concerning the interpretation of this QV-CP, including the definitions of capitalized terms, are set out in Appendix A hereto.

The provisions of this QV-CP are deemed incorporated in and to form part of each User Agreement unless expressly excluded or modified thereby. Without limitation to the generality of the foregoing, persons choosing to use Certificates or to rely on Certificates (in circumstances where they are authorised to do so) within the QV-PKI are deemed to have accepted the terms and conditions of such use or reliance including, without limitation, the terms and conditions of the then applicable User Agreement. Accordingly, the use of and reliance on Certificates within the QV-PKI assumes acceptance of and compliance with the terms and conditions applicable to those Certificates including, without limitation to the generality of the foregoing, the provisions of this QV-CP and applicable User Agreement as the same may, from time to time, be amended or supplemented.

1.2. Certificate Types

QuoVadis, in its capacity as the QuoVadis Root Certificate Authority (QV-RCA), has issued itself with the Root CA Certificate. The QV-RCA represents the apex of the QV-PKI and the Root CA Certificate enables the QV-RCA to digitally sign QV Issuing CA Certificates. Certificates are issued to (i) QV Issuing CAs, (ii) QuoVadis Registration Authorities (QV-RAs), (iii) QuoVadis Registration Authority Operators (QV-RAOs), (iv) QV Corporate Registration Authorities (QV-CRA), (v) Individuals and (vi) Organisations, in connection with the Identification and Authentication of Devices. For the purposes of this QV-CP, Certificates, other than the Root CA Certificate, are described under the following headings:

1.2.1.1. Utility Certificates

QV Issuing CA Certificate – The QV-RCA generates and issues QV Issuing CA Certificates, which are used by QV Issuing CAs to digitally sign and issue Certificates to Individuals or Devices.

QV-RA Certificate – QV Issuing CAs that are authorized to do so may generate and issue QV-RA Certificates, which are used to designate a QV-RA.

QV-RAO Certificate – QV Issuing CAs that are authorized to do so may issue QV-RAO Certificates to Individuals, that designate those Individuals as being authorized to perform QV-RA functions within a particular QV-RA.

QV-CRA Certificate – QV Issuing CAs that are authorized to do so may generate and issue QV-CRA Certificates, which are used to designate one or more individuals within an Organisation as authorized to administer User Certificates.

1.2.1.2. User Certificates

The following Certificate types are supported under this QV-CP:

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 may be described in outline as follows:

QV1 Certificate: Issued to Individuals based on identity and related information self-certified by the Applicant; designated as a Low Reliance Certificate.

QV2 Certificate: Accredited Certificate under the Bermuda CSP Legislation, issued to Individuals based on certified true copies of documents that support the claimed Identity of the Applicant or that Applicant's in person appearance before the relevant QV-RA; designated as a High Reliance Certificate.

QV3 Certificate: Accredited Certificate under the Bermuda CSP Legislation issued to the Applicant based on the Applicant's employment relationship with the QV-RA, QV-CRA, or Sponsoring Organisation (or their respective Subsidiaries and Holding Companies) responsible for the Certificate application or that Applicant's pre-existing relationship; designated as a Low Reliance Certificate.

QV4 Certificate: Accredited Certificate under the Bermuda CSP Legislation issued to the Applicant based on the Applicant's employment relationship with the QV-RA, QV-CRA, or Sponsoring Organisation (or their respective Subsidiaries and Holding Companies) responsible for the Certificate application or that Applicant's pre-existing documented relationship established in accordance with recognised Know-Your-Customer standards with the QV-RA, QV-CRA, or Sponsoring Organisation (or their respective Subsidiaries and Holding Companies) responsible for the Certificate application; designated as a High Reliance Certificate.

Device Certificate: QV Issuing CAs authorized to do so may generate and issue Device Certificates. Device Certificates are used to identify and Authenticate Secure Socket Layer or Virtual Private Network enabled devices.

Additional Certificates

In addition to the QV Type Certificates and Device Certificates described above, QuoVadis may permit the issuance of additional types of Certificates. QuoVadis may act as the Certificate Authority for certain communities of Users that require Certificates to be issued and managed within a defined and generally closed community. These Certificates may be described and identified within the body of this QV-CP or as a schedule hereto. Matters specific to those Certificate types, that may include Identification and Authentication requirements, warranty levels, and scope of use, will be separately identified. In all other respects, the management and operation of those Certificate types will be governed by the terms of this QV-CP. In addition,

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 QV-CP.

1.2.1.4. Certificate Profiles

Certificate Profiles for all Certificates supported by this QV-CP are attached as Appendix C to this QV-CP.

1.3. Identification

1.3.1. Object Identifiers

The Private Enterprise object identifier (OID) assigned by the Internet Assigned Numbers Authority (IANA) to QuoVadis is 1.3.6.1.4.1.8024.0.

The OID assigned to the Root CA Certificate is 1.3.6.1.4.1.8024.0.1

The OID assigned to this QV-CP is 1.3.6.1.4.1.8024.0.1.2000.1.2

OID assignment for the documentation of individual Certificate profile values is determined by their location in the CP Appendix, and each new Certificate profile OID will increment in value as new profiles are chronologically assigned and documented for new certificate types.

1.4. Community and Applicability

The use of Certificates supported by this QV-CP is restricted to parties authorised by contract to do so. Persons and entities other than those authorised by contract may not use Certificates for any purpose. No reliance may be placed on a Certificate by any Person unless that Person is an Authorised Relying Party.

A Certificate does not convey evidence of authority of an Individual to act on behalf of any person or to undertake any particular act and Authorised Relying Parties are solely responsible for exercising due diligence and reasonable judgement before choosing to place any reliance whatsoever on a Certificate. A Certificate is not a grant, assurance, or confirmation from QuoVadis or any QV-Provider of any authority, rights, or privilege save as expressly set out in this QV-CP.

Certificates may not be used and no participation is permitted in the QV-PKI (i) in circumstances that breach, contravene, or infringe the rights of others or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order in Bermuda or (iii) in connection with fraud, pornography, obscenity, hate, defamation or harassment.

Any person participating within the QV-PKI irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this QV-CP shall occur and shall be deemed to occur in Bermuda and that the performance of QuoVadis' obligations hereunder shall be performed and be deemed to be performed in Bermuda.

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 the provisions of this QV-CP. QV-CRAs will be provided with software and know-how to permit the provision of Certificates directly within the QV-PKI.

1.4.6. Sponsoring Organisations

Organisations may become Sponsoring Organisations within the QV-PKI. Sponsoring Organisations may only request the issue of QV4 Certificates to their employees and may request the issue of QV2 Certificates and QV3 Certificates to Affiliated Persons. Sponsoring Organisations are required to perform Identification and Authentication requirements for their employees and Affiliated Persons and to fulfil their functions pursuant to a Sponsoring Organisation Agreement with QuoVadis and to comply with the provisions of this QV-CP. Sponsoring Organisations submit the relevant Certificate applications and supporting

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 Users or Subscribers of QV Certificates are automatically deemed Authorised Relying Parties.

1.4.9. Applicability

This QV-CP is applicable to all Certificates issued by the QV-RCA and by QV Issuing CAs. Certificates issued under this QV-CP are intended to support secure electronic commerce and the secure exchange of information by electronic means. Certificates may be employed for identification, providing data confidentiality and data integrity, and for creating digital signatures. No reliance may be placed on Certificates and Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use (ii) in breach of this QV-CP or the relevant User Agreement (iii) in any circumstances where the use of Certificates could lead to death, injury, or damage to property; or (iv) as otherwise may be prohibited by the terms of issue.

1.5. Contact Details

This QV-CP is developed, administered, and maintained by QuoVadis through the QV-PMA. Questions and comments regarding this QV-CP should be addressed to:

QuoVadis Limited
Suite 1640,
48 Par-La-Ville Road,
Hamilton HM-11,
Bermuda

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

2. General Provisions

2.1. Obligations

This section details the obligations of QuoVadis, all QV Issuing CAs, QV-RAs, QV-CRAs and Sponsoring Organisations, Subscribers, and Authorised Relying Parties.

2.1.1. QuoVadis Obligations

QuoVadis is obligated to operate the QV-RCA and QV-CA in accordance with this QV-CP and other relevant operational policies and procedures with respect to the issuance and management of Certificates.

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.

2.1.2.7. Operations

QV Issuing CAs are required to ensure that administrative procedures related to personnel and procedural requirements, and physical and technological security mechanisms, are maintained in accordance with this QV-CP and other relevant operational documents.

2.1.2.8. Compliance

QV Issuing CAs must comply with the provisions of a QV Issuing CA Agreement, and this QV-CP including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements..

2.1.2.9. Privacy Policy

QV Issuing CAs are required to publish and follow a privacy policy in accordance with this QV-CP and applicable QV Issuing CA Agreement.

2.1.3. QV-RA Obligations

Whenever QuoVadis or a QV Issuing CA designates a QV-RA, the QV-RA is obligated to perform certain functions pursuant to a QV-RA Agreement including the following:

2.1.3.1. Certificate Applications

Process Certificate application requests in accordance with this QV-CP and applicable QV-RA Agreement, and other policies and procedures with regard to the Certificates issued.

2.1.3.2. Records

Maintain and process all supporting documentation related to the Certificate application process.

2.1.3.3. Revocation

Process Certificate Revocation requests in accordance with this QV-CP, applicable QV-RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued.

2.1.3.4. Privacy Policy

Publish and follow a privacy policy in accordance with this QV-CP and applicable QV-RA Agreement.

2.1.3.5. Compliance

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

2.1.4. QV-CRA Obligations

Whenever QuoVadis or a QV Issuing CA designates a QV-CRA, the QV-CRA is obligated to perform certain functions pursuant to a QV-CRA Agreement including the following:

2.1.4.1. Certificate Applications

Process Certificate application requests in accordance with this QV-CP and applicable QV-CRA Agreement, and other policies and procedures with regard to the Certificates issued.

2.1.4.2. Records

Maintain and process all supporting documentation related to the Certificate application process.

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 procedures required in connection with the Identification and Authentication requirements relevant to the Certificate issued.

2.1.6.3. Review of Certificate Information

Review the Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the QV Issuing CA or the Subscriber's QV-RA, QV-CRA, or Sponsoring Organisation, as the case may be, immediately in the event that the Certificate contains any inaccuracies.

2.1.6.4. Generation of Public/Private Key Pair

Generate a Key Pair, and promptly review, verify and accept or reject the information contained in the Certificate signed by the Issuing CA.

2.1.6.5. Security

Secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised use of their Private Key (to include password, hardware token, or other activation data used to control access to the Subscriber's Private Key).

Exercise sole and complete control and use of the Private Key that corresponds to the Subscriber's Public Key included in the Certificate issued to them.

Immediately notify the QV Issuing CA, and the Subscriber's QV-RA, QV-CRA, or Sponsoring Organisation, as the case may be, in the event of the compromise of its Private Key, such obligation to extend to notification to the QV Issuing CA, and the Subscriber's QV-RA, QV-CRA, or Sponsoring Organisation, as the case may be, in the event that the Subscriber has reason to believe or suspects or ought reasonably to suspect that its 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 QuoVadis or the QV-PKI.

2.1.6.6. Use of Certificates

At all times utilise its Certificate in accordance with this QV-CP and all applicable laws and regulations.

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

2.1.7. Authorised Relying Party Obligations

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

An Authorised Relying Party shall not place reliance on a 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 its Relying Party Agreement.

For the purposes of this QV-CP, the term "Reasonable Reliance" shall mean:

(i) that the attributes of the Certificate relied upon are appropriate in all respects to the reliance placed upon that 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 Certificate relied upon; (it being understood that QV1 Certificates represent the lowest level of Identification and Authentication and QV4 Certificates represent the highest level of Identification and Authentication applicable to Certificates);

(ii) that the Authorised Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted under this QV-CP;

(iii) 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;

(iv) that the 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 Certificate in accordance with the provisions of this QV-CP;

(v) that the Authorised Relying Party has, at the time of that reliance, verified the Digital Signature, if any; and

(vi) 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 Certificate being relied upon.

2.2. Liability

2.2.1. No Warranty

QuoVadis and QV Providers make no express or implied representations or warranties pursuant to this QV-CP. QuoVadis expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose.

2.2.2. Limitation of Liability

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

For the avoidance of doubt, QuoVadis shall bear no liability or responsibility to any person that participates in the QV-PKI unless that person is a Holder.

2.2.2.1. Certificate Loss Limits

Without prejudice to any other provision of this Section 2, QuoVadis' liability for breach of its obligations pursuant to this QV-CP shall, absent fraud or wilful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below.

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 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;

b) Power failure, power interruption, or other disturbances to electrical power, provided QuoVadis uses commercially reasonable methods to protect against such disturbances;

c) 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

d) 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.

2.2.2.3. Exclusions specific to Certificates

Notwithstanding any other provisions of this Section 2, QuoVadis shall bear no liability for loss involving or arising out of or relating to the use of a Certificate or any services provided by QuoVadis with respect to Certificates in circumstances where such loss arises from any one (or more) of the following circumstances or causes:

a) If the 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 Certificate or any password or activation data used to control access thereto;
b) If the 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;
c) If the 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;
d) If the 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 QV-CP and/or the relevant User Agreement or any applicable law or regulation;
e) If the Private Key associated with the Certificate held by the claiming party or otherwise the subject of any claim has been compromised; or
f) If the Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation.

2.2.3. Claims Procedure

Claim Request
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 Certificate held by the claiming party.

Further Assurances
As a precondition to QuoVadis' payment of any claim under the terms of this QV-CP, 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.

2.3. Financial Responsibility

2.3.1. Indemnification

Indemnification obligations may be contained in QV Issuing CA Agreements, QV-RA Agreements, QV-CRA Agreements, and Relying Party Agreements and other agreements. QV Providers (including QuoVadis) may enter into indemnification agreements to appropriately allocate risks and financial responsibility as a result of their respective roles and responsibilities within the QV-PKI.

2.3.2. Fiduciary Relationships

Issuance of Certificates and/or any participation within the QV-PKI does not make any QV Provider (including QuoVadis) an agent, fiduciary, trustee, or other representative of any person, whether a User or otherwise. Nothing contained in this QV-CP or in a User Agreement shall be deemed to constitute QuoVadis, any QV Provider, or any of its or their agents, directors, employees, consultants, suppliers, contractors, partners, or affiliates a fiduciary, endorser, promoter, agent, partner, representative, or affiliate of any person, whether a User or otherwise, and the use of or reliance on Certificates or other participation within the QV-PKI is to be construed accordingly.

2.3.3. Maintenance of Financial Records

QuoVadis and each QV Issuing CA within the QV-PKI is responsible for maintaining its financial books and records in a commercially reasonable manner. Each QV Issuing CA shall also employ

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 conferred upon it by this QV-CP; shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of this QV-CP is intended to be exclusive of any other right or remedy, except as expressly provided in this QV-CP, and each and every right or remedy shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

2.4.5. Dispute Resolution

Any controversy or claim between two or more participants in the QV-PKI (for these purposes, QuoVadis shall be deemed a “participant within the QV-PKI”) arising out of or relating to this QV-CP shall be shall be referred to an arbitration tribunal in the manner hereinafter set out:

(i) The arbitration will be conducted in accordance with the procedures set out in this QV-CP and the Bermuda International Conciliation and Arbitration Act (1993), as the same may

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 or equitable relief of any sort. They shall have no power to award punitive damages or any other damages not measured by the prevailing party's actual damages, and the parties expressly waive their right to obtain such damages in arbitration or in any other forum. In no event, even if any other portion of these provisions is held to be invalid or unenforceable, shall the arbitrators have power to make an award or impose a remedy that could not be made or imposed by a court deciding the matter in the same jurisdiction.

(v) No discovery will be permitted in connection with the arbitration unless it is expressly authorized by the arbitration panel upon a showing of substantial need by the party seeking discovery.

(vi) All aspects of the arbitration shall be treated as confidential. Neither the parties nor the arbitrators may disclose the existence, content or results of the arbitration, except as necessary to comply with legal or regulatory requirements. Before making any such disclosure, a party shall give written notice to all other parties and shall afford such parties a reasonable opportunity to protect their interests.

(vii) The result of the arbitration will be binding on the parties, and judgment on the arbitrators' award may be entered in any court having jurisdiction.

(viii) All costs of the arbitration shall be determined by the arbitration tribunal who may, taking into account the law and practice of the place of arbitration, direct to and by whom and in what manner they shall be paid.

(ix) Unless all parties agree to an alternative venue, any mediation or arbitration conducted pursuant to this section shall take place in Bermuda.

2.4.6. Fees

Detailed information related to fees charged to Subscribers and Authorised Relying Parties is required to be made known to Subscribers and Authorised Relying Parties. Fees may be levied in connection with the following:

(i) Certificate issuance, revocation, and renewal;
(ii) Private Encryption Key Archive and recovery;
(iii) Certificate status and Validation;
(iv) Policy access fees.

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

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

2.6.2. QV-RAs, QV-CRAs and Sponsoring Organisations

Each QV-RA, QV-CRA, and Sponsoring Organisation will be 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 QV-PKI. The obligations of QV-CAs, QV-CRAs, and Sponsoring Organisations within the QV-PKI are established by contract between those entities and QuoVadis.

2.6.2.1. Actions Taken as a Result of Deficiency

If irregularities are found, QuoVadis will address the issues raised with the relevant entity. Any action to be taken will be determined by QuoVadis by reference to its determination as to the severity or materiality of the irregularity. In the event that QuoVadis determines that remedial action is required, the relevant entity will be advised by QuoVadis as to the procedures and action required to remedy the irregularity. Remedial action determined by QuoVadis shall be limited to the operations and procedures required to be taken in order to ensure that the QV-RA, QV-CRA or Sponsoring Organisation operates in compliance with the QV-CP. In the event that QuoVadis determines that remedial action is required, and such action is not taken in accordance with QuoVadis' determination, QuoVadis may (i) allow the QV-CA, QV-CRA, or Sponsoring Organisation to continue operations for a further period of time whilst those irregularities are addressed; (ii) allow the QV-CA, QV-CRA or Sponsoring Organisation to continue operations for a maximum of thirty (30) days pending full implementation of the actions required by QuoVadis prior to termination of that QV-CA's, QV-CRA's, or Sponsoring Organisation's agreement with QuoVadis and the associated revocation of any Certificate issued to them; (iii) limit the class of any Certificates issued by the QV-CA, QV-CRA or Sponsoring Organisation; or (iv) terminate that QV-CA's, QV-CRA's or Sponsoring Organisation's agreement with QuoVadis and revoke any Certificate issued to them in that capacity. Any decision regarding which of these actions to take will be based on QuoVadis' opinion of the severity and materiality of the irregularities.

2.7. Confidentiality

QuoVadis does not have access to the Private Keys of any of the entities it certifies or whose certification requests it processes. There is no requirement to place a copy of any Private Key with any backup/recovery or escrow service. Under contract between a Subscriber, CRA, or Sponsoring Organisation and QuoVadis, a copy of an entity's encryption Keys may be archived by QuoVadis for possible retrieval of encrypted information upon the loss or corruption of the original encryption Keys.

2.7.1. Types of Information to be Kept Confidential

Any personal or corporate information held by any QV Issuing CAs, QV-RAs or QV-CRAs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant Holder, unless required otherwise by law or to fulfil the requirements of this QV-CP.

2.7.2. Types of Information Not Considered Confidential

Information appearing on Certificates or stored in the Repository is not considered confidential, unless statutes or special agreements so dictate.

2.7.3. Disclosure of Certificate Revocation Information

Certificate revocation information is provided via the CRL in the QuoVadis X.500 Directory services.

2.7.4. Release to Law Enforcement Officials

As a general principle, no document or record belonging to QuoVadis is released to law enforcement agencies or officials except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to QuoVadis to be under appeal when served on QuoVadis (QuoVadis being under no obligation to determine the same), and which has been determined by the Supreme Court of Bermuda to be valid, subsisting, issued in accordance with general principles of Bermuda law and otherwise enforceable in Bermuda.

2.7.5. Release as Part of Civil Discovery

As a general principal, no document or record belonging to QuoVadis is released to any person except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to QuoVadis to be under appeal when served on QuoVadis (QuoVadis being under no obligation to determine the same), and which has been determined by the Supreme Court of Bermuda to be valid, subsisting, issued in accordance with general principles of Bermuda law and otherwise enforceable in Bermuda.

2.8. Intellectual Property Rights

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

This QV-CP and the Proprietary Marks are the intellectual property of QuoVadis.

2.8.1. Copyright

QuoVadis retains exclusive title to, copyright in, and the right to license this QV-CP.

3. Identification and Authentication

3.1. Initial Registration

3.1.1. Responsibility for Identification and Authentication

QV Issuing CAs may perform the Identification and Authentication required in connection with the issue of Certificates, or they may delegate the responsibility to one or more QV-RAs. QV-CRAs and Sponsoring Organisations may perform the Identification and Authentication required in connection with the issue of QV3 and QV4 Certificates to their employees. In addition, QV-CRAs

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 Distinguished Name (DN). The Distinguished Name includes the following fields:

- Common Name (CN)
- Organisational Unit (OU)
- Organisation (O)
- Locality (L)
- State or Province (S)
- Country (C)
- Email Address (E)

The Common Name may contain the applicant's first and last name (surname). The Common Name, the Organisation and the Organisational Unit (where applicable) are the only fields authenticated during the Registration procedure. The User may choose whether to include the Locality, State and Country but they are not verified in any way. Such attributes do not necessarily indicate the subscriber's country of citizenship, country of residence, or the country of issuance of the certificate.

3.1.3. Need for Names to Be Meaningful

The contents of the Certificate Subject and 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 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 name of the Organisation responsible for that Device.

3.1.4. Uniqueness of Names

The Subject Name of each Certificate issued by a QV Issuing CA shall be unique for all Certificates issued by that QV Issuing CA and shall conform to all applicable X.500 standards for the uniqueness of names. The QV Issuing CA may, if necessary, insert additional numbers or letters to the Certificate subject's common name in order to distinguish between two Certificates that would otherwise have the same Subject Name.

3.1.5. Use of Names and Trademarks

QV Issuing CAs are not obligated to seek evidence of trademark usage by any Organisation.

3.1.6. Method to Prove Possession of Private Key

The QV Issuing CA shall establish that each Applicant for a Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the Certificate application. The QV Issuing CA shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol.

3.1.7. Identification and Authentication

This Section 3.1.7 describes the basis upon which Identification and Authentication is conducted in connection with the issuance of Certificates. This Section 3.1.7 is to be read in conjunction with Appendix B to this QV-CP (Certificate Characteristics) that sets out with respect to QV Type Certificates, in more detail, the information and documentation that is required, where relevant, to

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 Identity of an Organisation, at a minimum, confirmation is required that: (i) the Organisation legally exists in the name that will appear in the Organisational Unit (OU) field of any Certificates issued under its name, or routinely does business under an alternative OU identifier proposed by the Organisation; and (ii) all other information contained in the Certificate application is correct.

Registration information provided by an Organisation may be validated by reference to official government records and/or information provided by a reputable vendor of corporate information services. The accuracy and currency of such information may be validated by conducting checks with financial institution references, credit reporting agencies, trade associations, and other entities that have continuous and ongoing relationships with the Organisation under review. In addition, the telephone number provided by the Organisation as the telephone number of its principal place of business may be called to ensure that the number is active and answered by the Organisation.

Where a QV Issuing CA, QV-RA, QV-CRA, or Sponsoring Organisation has a separate and pre-existing commercial relationship with the Organisation under review, the QV Issuing CA, QV-RA, QV-CRA, or Sponsoring Organisation may Authenticate the Identity of the Organisation by reference to records kept in the ordinary course of business that, at a minimum, satisfy the requirements of this section. In all such cases, the QV Issuing CA, QV-RA, QV-CRA, or Sponsoring Organisation shall record the specific records upon which it relied for this purpose.

3.1.7.2. Employees

Where a QV Issuing CA issues QV3 and QV4 Certificates directly to employees of an Organisation, it shall, at least with respect to the first such Certificate issued to an employee of that Organisation, (i) conduct the Identification and Authentication of the Organisation in accordance with Section 3.1.7.1 and (ii) enter into a QV-RA Agreement, QV-CRA Agreement, or Sponsoring Organisation Agreement with that Organisation. The QV Issuing CA shall conduct the Identification and Authentication of individual employees of the Organisation in accordance with the applicable QV-RA Agreement, QV-CRA Agreement, or Sponsoring Organisation Agreement which shall set forth appropriate Identification and Authentication procedures for that QV-RA, QV-CRA, or Sponsoring Organisation. Those procedures shall require, at a minimum, either that (i) the QV Issuing CA Authenticates the identify of the employee by reference to at least one form of government-issued photographic identification; or (ii) the QV-RA, QV-CRA, or Sponsoring Organisation has, on at least one occasion during the person's employment with the QV-RA, QV-CRA or Sponsoring Organisation, Authenticated the Identity of the employee by reference to at least one form of government-issued photographic identification, and maintains business records of that fact.

3.1.7.3. Affiliated Persons

A QV-RA, QV-CRA, or Sponsoring Organisation approving the issuance of a QV3 or QV4 Certificate to an Affiliated Person may Authenticate the Identity of the Affiliated Person by reference to business records maintained by the QV-RA, QV-CRA, or Sponsoring Organisation,

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 (including copies of required identification) is received by mail or electronic methods, such information must be obtained directly from (i) a known and reputable financial institution that is subject to Know-Your-Customer requirements in a jurisdiction that adheres to internationally-accepted principles against money laundering, such as those promulgated by the Financial Action Task Force on Money Laundering and the Bank for International Settlements; (ii) an affiliate or subsidiary of the QV Issuing CA that has previously established the Identity of the Applicant on the basis of in-person presentation of the required identification; or (iii) a notary or other person who is authorised under the law of the applicant's jurisdiction to Authenticate true and accurate copies, and who has Authenticated the applicant's registration information on the basis of an in-person presentation of that information.

3.1.8. Authentication of a Device

A QV Issuing CA may issue a Device Certificate to an Organisation that has been previously Authenticated in accordance with Section 3.1.7.1. The Organisation shall be responsible for establishing the Subject Name of the Device.

3.2. Certificate Rekey, Renewal and Update

QV Issuing CAs in the QV-PKI may not re-key, renew, or update existing Certificates. All Certificates must be renewed or modified by following the initial application process.

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 to be bound by contract with respect to the use of that Certificate. These contracts may be directly between the QV Issuing CA and the Holder or imposed upon that Holder through terms and conditions binding upon him. All agreements concerning the use of, or reliance upon, Certificates issued within the QV PKI must incorporate by reference the requirements of this QV-CP as it may be amended from time to time.

4.2. Certificate Issuance

4.2.1. QV-RCA

The Root CA Certificate has been self-generated and self-signed.

4.2.2. QV Issuing CA Certificates

Upon the acceptance of the terms of the QV Issuing CA Agreement by the QV Issuing CA, successful completion of the QV Issuing CA application process as prescribed by QuoVadis, and final approval of the application by the QV-RCA, the QV-RCA issues the QV Issuing CA Certificate to the relevant QV Issuing CA.

4.2.3. QV-RA Certificates

Upon the acceptance of the terms of a QV-RA Agreement, successful completion of the QV-RA application process and final approval of the application by the QV Issuing CA, the QV Issuing CA issues the QV-RA Certificate to the relevant QV-RA.

4.2.3.1. QV-RAO Certificates

As part of the application process, QV-RAs are required to nominate one or more persons within their Organisation to take responsibility for the operation of that Organisation QV-RA functions. Those nominated persons will each be issued with a QV-RAO Certificate.

4.2.4. QV-CRA Certificates

Upon the acceptance of the terms of a QV-CRA Agreement, successful completion of the QV-CRA application process and final approval of the application by the QV Issuing CA, the QV Issuing CA issues the QV-CRA Certificate to the relevant QV-CRA.

4.2.4.1. QV-CRAO Certificate

As part of the application process, QV-CRAs are required to nominate one or more persons within their Organisation to take responsibility for the operation of that Organisation's QV-CRA functions. Those nominated persons will each be issued with a QV-CRAO Certificate.

4.2.5. User Type Certificates

Upon the acceptance of the terms of a User Agreement or other relevant agreement by the Applicant, successful completion of the application process and final approval of the application by the QV Issuing CA, the QV Issuing CA issues the Certificate to the Applicant or Device.

4.3. Certificate Acceptance

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

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for Revocation

QuoVadis may revoke certificates issued to a QV Issuing CA at any time in its sole and absolute discretion. QV Issuing CAs shall revoke Certificates whenever:

(i) The QV Issuing CA becomes aware that any of the information in the Certificate has changed or become obsolete;
(ii) The QV Issuing CA becomes aware that the Holder has failed to meet its obligations under this QV-CP or any other agreement, regulation, or law that may be in force with respect to that Certificate;
(iii) The QV Issuing CA becomes aware that the Private Key associated with the Certificate is compromised or suspected to be compromised. (Key compromise includes suspected unauthorised access or suspected unauthorised access to Private Keys or any password or activation data used to control access to a Private Key, lost or suspected lost Keys, stolen or suspected stolen Keys, or destroyed Keys);
(iv) The QV Issuing CA is requested to revoke a Certificate by the Holder of that Certificate (or responsible person in the case of a Device Certificate);

(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 this QV-CP or an equivalent method.

4.4.4. Revocation Request Grace Period

No grace period is allowed once a revocation request has been verified. QV Issuing CAs will revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.4.5. Circumstances for Suspension

The QV-PKI does not support Certificate Suspension.

4.4.6. CRL Issuance Frequency

The QV-RCA and QV Issuing CAs will update their respective CRLs at the time of each Certificate Revocation.

4.4.7. CRL Checking Requirements

When a QV Issuing CA provides CRLs as a method of verifying the validity and status of Certificates, the following requirements will apply:

(i) Authorised Relying Parties who rely on a CRL must in their validation requests check a current, valid CRL for the QV Issuing CA in the Certificate path and obtain a current CRL; and
(ii) •Authorised Relying Parties who rely on a CRL must (i) check for an interim CRL before relying on a Certificate, and (ii) log their validation requests.

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

4.5. Security Audit Procedures

4.5.1. Types of Events Recorded

The QV-CA will log, for audit purposes, the creation of accounts (privileged or not), installation of new software or software updates, time and date and other descriptive information about all backups, shutdowns and restarts of the system, time and date of all hardware upgrades, time and date of audit log dumps, and time and date of transaction archive dumps. Audit logs will be appropriately integrity and time-stamp protected. All entries will be individually time stamped.

Audit trails must be implemented and maintained in order to record automatically all relevant electronic system activity resulting from the operations of each QV Issuing CA. Electronic system activity shall include at a minimum: logins; file access; requests for Certificates; Key generation requests; issuance of a Certificate; and all transactions related to Certificate status updates.

4.5.2. Frequency of Processing Log

Audit logs are verified and consolidated at least monthly.

4.5.3. Retention Period for Audit Log

Audit logs are retained as archive records for a period no less than 7 (seven) years for audit trail files, and no less than 10 (ten) years for Key and Certificate information.

Audit logs are stored until at least 7 (seven) years after the QV Issuing CA ceases operation.

4.5.4. Protection of Audit Log

Only Certificate Authority Operators (CAO) 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 Certificate generated especially for the purpose of protecting the logs.

4.5.5. Audit Log Backup Procedures

Each QV 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 QV Issuing CA's premises and storage at a secure off-site (but readily available) location.

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.

4.7. Key Changeover

QuoVadis and each QV Issuing CA shall specify its Key changeover process in its policies and procedures. The process shall provide for a period of overlap between the old and new QV Issuing CA Keys.

4.8. Compromise and Disaster Recovery

QuoVadis and each QV Issuing CA has in place an appropriate disaster recovery and business resumption plan, which provides for immediate continuation of Certificate revocation services in the event of an unexpected emergency. QuoVadis regards its disaster recovery and business resumption plan as proprietary and that it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.
QuoVadis and each QV Issuing CA has in place an appropriate Key compromise plan detailing its activities in the event of a compromise of a QV Issuing CA Private Key. Such plans include procedures for:

(i) Revoking all Certificates signed with that QV Issuing CA's Private Key; and
(ii) Promptly notifying QuoVadis and all of the Holders of Certificates issued by that QV Issuing CA.

4.9. QV Issuing CA Termination

QuoVadis and each QV Issuing CA specifies the procedures it will follow when terminating all or a portion of its Certificate issuance and management operations. The procedures must, at a minimum:

(i) ensure any disruption caused by the termination of a QV Issuing CA is minimized;
(ii) ensure that archived records of the QV Issuing CA are retained;
(iii) ensure that prompt notification of termination is provided to Subscribers, Authorised Relying Parties, and other relevant parties; and
(iv) ensure that a process for revoking all Certificates issued by that QV Issuing CA at the time of termination is maintained.

In the event of the need for revocation of a QV Issuing CA's Certificate, that QV Issuing CA must immediately notify: (i) the PMA; (ii) all QV Issuing CAs to whom it has issued cross-certificates; (iii) all of its QV-RAs; (iv) all of its QV-CRAs; (v) all of its Sponsoring Organisations; (vi) all Holders of Certificates issued by it; and (vii) all Individuals or Organizations who are responsible for a Certificate issued by it to a Device. That QV Issuing CA must also: (i) publish the QV Issuing CA Certificate serial number on an appropriate CRL; and (ii) revoke all cross-Certificates signed with the revoked QV Issuing CA Certificate. After addressing the factors that led to revocation that QV Issuing CA may: (i) generate a new QV Issuing CA signing Key Pair; and (ii) re-issue Certificates and ensure all CRLs are signed using the new Key.

5. Security Controls

5.1. Physical Controls

Each QV Issuing CA specifies and implements appropriate physical security controls to restrict access to the hardware and software used in connection with their operations wherever those operations physically occur, including the QV Issuing CA's own physical facilities and those where its outsourced services occur.

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

recipient, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in PKCS#12) will be used. The resulting file may be kept on a magnetic medium or transported electronically.

6.1.3. Public Key Delivery to Certificate Issuer

Public Keys must be delivered in a secure and trustworthy manner, such as a Certificate request message. Delivery may also be accomplished via non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a Token for local Key generation at the point of Certificate issuance or request. Off-line means will include Identity checking and will not inhibit proof of possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a User Agreement or other agreement. In those cases where Key Pairs are generated by the QV Issuing CA on behalf of the Holder, the QV Issuing CA will implement secure mechanisms to ensure that the Token on which the Key Pair is held is securely sent to the proper Holder, and that the Token is not activated prior to receipt by the proper Holder.

6.1.4. QV Issuing CA Public Key Delivery to Users

Public Keys of QuoVadis and each QV Issuing CA shall be publicly available.

6.1.5. Key Sizes

The QV-CA uses an RSA minimum key length of 1,024 bit modulus.

6.1.6. Hardware/Software Key Generation

All Keys for QV Issuing CAs, QV-RAs, QV-RAOs, QV-CRAs, and QV-CRAOs must be randomly generated in a Token. Any pseudo-random numbers used for Key generation material will be generated by an FIPS approved method.

6.1.7. QV Issuing CA Key Usage Purposes

The QV Issuing CA Private Key is used for Certificate signing and CRL signing. It may also be used to Authenticate the QV Issuing CA to the Repository.

6.2. Private Key Protection

All participants in the QV-PKI are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this QV-CP. Without limitation to the generality of the foregoing, all participants in the QV-PKI must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised use of their Private Key (to include password, Token or other activation data used to control access to the Private Key); and (ii) exercise sole and complete control and use of their Private Key that corresponds to their Public Key.

6.2.1. Standards for Cryptographic Module

Cryptographic modules in use with the QV-PKI comply with industry standards, FIPS – Level 4.

6.2.2. Private Key (n out of m) Multi-Person Control

The QV-PKI uses multi-person control for both access control and authorisation control.

6.2.3. Private Key Escrow

Private Keys shall not be escrowed.

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.

6.2.5. Private Key Archival

Private Keys used for encryption shall not be archived, unless the Subscriber, QV-CRA or Sponsoring Organisation specifically contracts for such services. Under no circumstances will the signing Keys be archived.

6.2.6. Private Key Entry into Cryptographic Module

In the event that a Private Key is to be transported from one Cryptomodule to another, the Private Key must be encrypted during transport. Private Keys must never exist in plain text form outside the Cryptomodule.

6.2.7. Method of Activating Private Key

A Subscriber must be Authenticated to the Cryptomodule before the activation of the Private Key. This Authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

6.2.8. Method of Deactivating Private Key

Cryptomodules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptomodules should be removed and stored, unless they are within the Holder's sole control.

6.2.9. Method of Destroying Private Key

Private Keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public Keys will be recorded in Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained.

6.3.2. Usage Periods for Public and Private Keys

Usage periods for Public Keys and Private Keys shall match the usage periods for the Certificate that binds the Public Key to an Individual, Organisation, or Device.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Two factor Authentication shall be used to protect access to a Private Key. One of these factors must be randomly and automatically generated.

If the activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptomodule.

6.4.2. Activation Data Protection

Activation Data should be memorized, not written down. Activation Data must never be shared.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

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

6.6. Life Cycle Technical Controls

All hardware and software procured for operating any QV Issuing CA within the QV-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 QV-PKI shall be developed in a controlled environment under strict change control procedures.

A continuous chain of accountability, from the location where all hardware and software that has been identified as supporting a QV Issuing CA within the QV-PKI, must be maintained by causing it to be shipped or delivered via controlled methods. The QV Issuing CA equipment shall not have installed applications or component software that are not part of the QV Issuing CA configuration. All subsequent updates to QV Issuing CA equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

6.7. Network Security Controls

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

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

6.8. Hardware Cryptomodule Engineering Controls

Cryptomodule used by the QV-RCA, QV-ICA, and QV-RAs are certified to Internet Engineering Task Force (IETF) Standards.

7. Certificate and CRL Profiles

7.1. Certificate Profile

As specified in the QuoVadis Certificate Profile Policy found in Appendix C to this QV-CP.

7.2. CRL Profile

If utilized, CRLs will be issued in the X.509 version 2 format. The applicable CPS or other publicly available document will identify the CRL extensions supported and the level of support for these extensions.

7.2.1. Version Number

QV Issuing CAs must issue X.509 version 2 CRLs in accordance with the PKIX Certificate and CRL Profile.

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 publicly available documents will identify and define the use of any extensions supported by QV Issuing CAs, QV-RAs, QV-CRAs, and Users.

8. Specification Administration

8.1. Specification Change Procedures

8.1.1. Changes without Notification

The only changes that may be made to this QV-CP without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the PMA, materially impact any participants within the QV-PKI.

8.1.2. Changes with Notification

In this paragraph "level of trust" does not include those parts of the specification relating to the liabilities of the parties. Reference to "level of trust" applies solely to the technical/administrative functions and any changes provided for under this clause shall not materially change this specification unless there is a significant business reason to do so.

Any change that increases the level of trust that can be placed in Certificates issued under this QV-CP or under policies that make reference to this QV-CP requires thirty (30) days prior notice.

Any change that decreases the level of trust that can be placed in Certificates issued under this QV-CP or under policies that make reference to this QV-CP requires forty-five (45) days prior notice. The QV-CP applicable to any Certificate supported by this QV-CP shall be the QV-CP currently in effect; no provision is made for different versions of this QV-CP to remain in effect at the same time.

The QV-PMA has authority to evaluate all changes and determine whether prior notification is required and whether the QV-CP OID should be changed.

8.2. Publication and Notification

Required notices of proposed changes to the QV-CP will be made via the QuoVadis web site at www.quovadis.bm.

Notice of proposed changes are recorded in the change log at the beginning of this QV-CP until they are approved, at which time the approved change will be recorded there permanently.

8.3. Change Approval Procedures

8.3.1. QV-PMA

The QV-PMA shall review all comments submitted regarding proposed changes and shall have authority to recommend changes following consultation with QuoVadis.

8.3.2. Approval Date

This QV-CP was approved on 1st March, 2004.

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;
"**Applicant**" means an Individual or Organisation that has submitted an application for the issue of a 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 Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.
"**Authentication**" means procedures followed or to be followed designed and intended to provide against fraud, imitation and deception ("Authenticate" and "Authenticated" to be construed accordingly);
"**CAO**" means a Certificate Authority Operator;
"**Certificate**" means a digital identifier within the QV-PKI that: (i) identifies the Certificate Authority issuing it; (ii) names or identifies a Holder or Device; (iii) contains the Public Key of the Holder; (iv) identifies the Certificate's Operational Term; (v) is digitally signed by a Certificate Authority; and (vi) has the meaning ascribed to it in accordance with the documentation that governs its issuance and use and includes the contents of that Certificate whether expressly included or incorporated by reference;
"**Certificate Authority**" **or** "**CA**" means an Organisation that creates, issues, revokes and otherwise manages Certificates;
"**Certificate Chain**" means a chain of multiple Certificates required to Validate a Certificate containing a Private Key typically consisting of a Certificate of a Public Key owner signed by one QV Issuing CA and one or more additional Certificates of QV Issuing CAs signed by other QV Issuing CAs;
"**Certificate Policy**" **or** "**QV-CP**" means this certificate policy adopted by QuoVadis as the same may, from time to time, be amended or supplemented containing a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements;
"**Certificate Practice Statement**" **or** "**CPS**" means a certificate practice statement setting out, in general terms, an overview of the QV-PKI, its operations and a QV Provider's practices within the QV-PKI;
"**Certificate Revocation**" means the process of removing a Certificate from the management system and indicating that the Key Pair related to that Certificate should no longer be used;
"**Certificate Revocation List**" **or** "**CRL**" means a signed list of Certificates that have been revoked by a QV Issuing CA and maintained by that QV Issuing CA;
"**Cryptomodule**" means secure software, device or utility that (i) generates Key Pairs; (ii) stores cryptographic information; and/or (iii) performs cryptographic functions;
"**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 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**" means a process to distinguish a subject or entity from other subjects or entities;
"**Identity**" means a set of attributes which together uniquely identify a subject or entity;
"**Identification**" means reliance on data to distinguish and Identify an entity or subject;
"**Identification and Authentication**" or "**I&A**" means the procedures and requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity;
"**Individual**" means a natural person;
"Key" means a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification);
"**Key Pair**" means two related Keys, one being a Private Key and the other a Public Key having the ability whereby one of the pair will decrypt the other;
"**Object Identifier**" or "**OID.**" means the unique identifier registered under the ISO registration standard to reference a specific object or object class;
"**Operational Term**" means the term of validity of a Certificate commencing on the date of its issue and terminating on the earlier of (i) the date disclosed in that Certificate or (ii) the date of that Certificate's Revocation;
"**Organisation**" means an entity that is legally recognised in its jurisdiction of domicile (and can include a body corporate or un-incorporate, partnership, trust, non-profit making Organisation, government entity);
"Proprietary Marks" means any patents (pending or otherwise), trade marks, trade names, logos, registered designs, symbols, emblems, insignia, fascia, slogans, copyrights, know-how, information, drawings, plans and other identifying materials whether or not registered or capable of registration and all other proprietary rights whatsoever owned by or available to QuoVadis adopted or designated now or at any time hereafter by QuoVadis for use in connection with the QV-PKI;
"**Private Key**" means a Key forming part of a Key Pair that is required to be kept secret and known only to the person that holds it;
"**Public Key**" means a Key forming part of a Key Pair that can be made public;
"**Public Key Infrastructure**" **or** "**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;
"**QuoVadis**" means QuoVadis Limited, a Bermuda exempted company;
"**QV-CA**" means QuoVadis in its capacity as a QV Issuing CA;
"**QV Corporate Registration Authority Operator**" or "**QV-CRAO**" means an Individual designated by a CRA as being authorized to perform the functions of that CRA;
"**QV Corporate Registration Authority**" **or** "**QV-CRA**" means an Organisation involved in verifying and enrolling participants in the QV-PKI;
"**QV-CPS**" means a CPS adopted by QuoVadis setting out, in general terms, an overview of the QV-PKI and its operations;
"**QV-CRA Certificate**" means a digital identifier issued by a QV Issuing CA in connection with the establishment of a QV-CRA within the QV-PKI;
"**QV Issuing CA**" means a CA (including QuoVadis in its capacity as a CA) duly authorised to operate by QuoVadis to issue certain Certificates within the QV-PKI;
"**QV Issuing CA Agreement**" an agreement entered into between QuoVadis and a QV Issuing CA (other than the QV-CA) pursuant to which that QV Issuing CA is to provide its services within the QV-PKI;
"**QV Issuing CA Certificate**" A Certificate issued by the QV-RCA to a QV Issuing CA enabling that QV Issuing CA to issue certain Certificates. A QV Issuing CA Certificate includes the Public

Key that corresponds to the QV Issuing CA's Private Key used in the management of Certificates issued by it within the QV-PKI;
"**QV-PMA**" means the QuoVadis Policy Management Authority;
"**QV-PMA Charter**" means the terms of reference adopted, from time to time, by the QV-PMA pursuant to which it performs its functions;
"**QV-PKI**" means the infrastructure implemented and utilized by QuoVadis for the generation, distribution, management and archival of Keys, Certificates and Certificate Revocation Lists and the Repository to which Certificates and Certificate Revocation Lists are to be posted;
"**QV Provider**" means a QV Issuing CA, a QV-RA, a QV-CRA;
"**QV-RA**" means an RA designated by a QV Issuing CA to operate within the QV-PKI;
"**QV-RA Agreement**" an agreement entered into between a QV Issuing CA and a QV-RA pursuant to which that QV-RA is to provide its services within the QV-PKI;
"**QV-RA Certificate**" means a digital identifier issued by a QV Issuing CA in connection with the establishment of a QV-RA within the QV-PKI;
"**QV-RAO**" means an RAO within a QV-RA;
"**QV-RCA**" means QuoVadis in its capacity as a Root Certificate Authority;
"**QV Registration Authority Operator**" or "**QV-RAO**" means an Individual designated by an RA as being authorized to perform the functions of that RA;
"**QV Registration Authority**" **or** "**QV-RA**" the part of a PKI involved in verifying and enrolling participants in that PKI;
"**Reasonable Reliance**" has the meaning set out in Section 2.1.7 of the QV-CP;
"Relying Party Agreement" means an agreement between QuoVadis and an Individual or Organisation setting forth the terms and conditions under which the Individual or Organisation is entitled to exercise Reasonable Reliance on Certificates.
"**Repository**" means one or more databases of Certificates and other relevant information maintained by QV Issuing CA's;
"**Responsible Person**" means an Individual(s), nominated by a Sponsoring Organisation, having responsibility for the performance of that Sponsoring Organisation's obligations pursuant to a Sponsoring Organisation Agreement;
"**Root CA Certificate**" means self-signed Certificate issued to the QV-RCA;
"**Root Certificate Authority**" or "**Root CA**" means QuoVadis as the source CA being a self-signed CA that signs QV Issuing CA Certificates;
"**Sponsoring Organisation**" means an Organisation that has entered into a Sponsoring Organisation Agreement;
"**Sponsoring Organisation Agreement**" means an agreement between a QV Issuing CA and an Organisation pursuant to which that Organisation participates within the QV-PKI;
"**Subscriber**" means a Holder that has been issued with a Certificate;
"**Token**" means a Cryptomodule consisting of a hardware object (e.g., a "smart card"), often with a memory and microchip;
"**User**" means a Holder or a person participating in the QV-PKI;
"**User Agreement**" means a contract between a User and QuoVadis that contains, expressly or by reference, the terms and conditions of use of the QV-PKI; and
"**Validation**" means an online check, by OCSP request, or a check of the applicable CRL(s) (in the absence of OCSP capability) of the validity of a Certificate and the validity of any Certificate in that Certificate's Certificate Chain for the purpose of confirming that the Certificate is valid at the time of the check (i.e., it is not revoked or expired).

Monetary values used in this policy are expressed as the lawful currency of the United States of America.

In this Agreement, words importing the singular include the plural and vice versa, words importing one gender include both genders and the neuter and references to persons include bodies corporate or unincorporate.

References in this Agreement to statutory provisions are references to those provisions as respectively amended or re-enacted from time to time (if and to the extent that the provisions as

amended or re-enacted are for the purposes hereof equivalent to those provisions before such amendment or re-enactment) and shall include any provision of which they are re-enactments (if and to the extent aforesaid) and any issuing legislation made under such provisions.

References herein to "Clauses", "Schedules", and "Annexures" are to clauses of and schedules and annexures to this Agreement respectively and a reference to this Agreement includes a reference to each Schedule and to any Annexures hereto.

The headings and table of contents in this Agreement are for convenience only and shall not affect its interpretation.

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)
Not Applicable	Not Applicable	Full name of Applicant:	Full name of Applicant:
Not Applicable	Not Applicable	Country	Country
Not Applicable	Not Applicable	E-mail address:	E-mail address:

IDENTIFICATION

QV1 Certificate	QV2 Certificate	QV3 Certificate for Trading Partners, Clients or Affiliates	QV4 Certificate for Employees
Not Applicable	Not Applicable	Existing Commercial Relationship	Human Resources Records including copy of Passport or other Government Identity Documentation or Existing Commercial Relationship together with completion of Know-Your-Customer requirements in a jurisdiction that adheres to internationally accepted principles against money laundering, such as those promulgated by the Financial Action Task Force on Money Laundering and the Bank for International Settlements;

OPTIONAL INFORMATION

QV1 Certificate	QV2 Certificate for Trading Partners, Clients or Affiliates	QV3 Certificate for Trading Partners, Clients or Affiliates	QV4 Certificate for Employees
Not Applicable	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.

AUTHENTICATION

QV1 Certificate	QV2 Certificate	QV3 Certificate	QV4 Certificate
Not Applicable	Not Applicable	Documentary Check	Documentary Check
Not Applicable	Not Applicable	Verify employment status/Ensure completeness and validity of Know-Your-Customer required Documentation	Verify employment status/Ensure completeness and validity of Know-Your-Customer required Documentation