CERTIFICATION PRACTICE STATEMENT - RCA

O.I.D: 1.3.6.1.4.1.8024.0.1.2000.1
Effective Date: August 1st 2003
Version: 2.06

Important Note About this Document

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

Contact
QuoVadis Limited
Cumberland House,
1 Victoria Street,
Hamilton HM-11,
Bermuda

Electronic mail: policy@quovadis.bm
Website: www.quovadis.bm
This document is controlled and managed under the authority of the PMA.

Version Control

	Date	Version	Description	Author
1	2002-2-28	2.05	Revised	QV PMA
2	2003-8-01	2.06	Revised for WebTrust	QV PMA
3				

Table of Contents

1. Introduction

1.1. Overview

The practices described in this Certification Practice Statement (CPS), together with the technologies, policies and procedures referred to in other documents produced and adopted by QuoVadis Limited (QuoVadis or QV) as further described herein, describe in outline the trustworthiness and integrity of the QV Root Certification Authority (QV-RCA) operations throughout the Certificate lifecycle, from Certificate application to revocation or expiry.

This CPS is written to provide a general overview of the use of all Certificates under the QuoVadis PKI Public Key Infrastructure (QV-PKI). The QV-PKI is designed and is operated to comply with the broad strategic direction of existing international standards for the establishment and operation of a Public Key Infrastructure Certification Authority. This CPS is not intended to create contractual relationships between QuoVadis and any other person. Any person seeking to rely on Certificates or participate within the QV-PKI must do so pursuant to definitive contractual documentation.

This CPS undergoes a regular review process and is subject to amendment as prescribed by the QV Policy Management Authority (PMA).

The structure of this CPS is based on Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, but does not seek to adhere or follow it exactly.

1.1.1. 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.

1.1.1.1. 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 an Organisation as 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 an Organisation as a QV-CRA.

1.1.1.2. 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. 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. Identification

1.2.1. Certificate Practice Statement

This Certificate Practice Statement is referred to as the CPS or QV-CPS.

1.2.2. Object Identifiers

The Object Identifier (OID) assigned to this CPS is 1.3.6.1.4.1.8024.6.

1.3. Community and Applicability

QuoVadis has established the QV-RCA under which a number of subordinate services operate. These subordinate services within the QV-PKI are either:

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

This CPS describes in outline all subordinate services that operate under the QV-RCA, i.e. that are within the QuoVadis “chain of trust”.

The practices described or referred to in this CPS:

- accommodate the diversity of the community and the scope of applicability within the QuoVadis chain of trust; and
- adhere to the primary purpose of the CPS, of describing the uniformity and efficiency of practices throughout the QV-PKI.

In keeping with their primary purpose, the practices described in outline in this CPS:

- are the minimum requirements necessary to ensure that Subscribers and Authorised Relying Parties have a high level of assurance, and that critical functions are provided at appropriate levels of trust; and
- apply to all stakeholders, for the generation, issue, use and management of all Certificates and Key Pairs.

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 or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy in Bermuda.

The QV-PMA has been established to maintain the integrity of the policy and procedure infrastructure adopted by QuoVadis. The PMA seeks to accomplish the foregoing through the adoption of various policies and procedures detailed in separate agreements and documentation. This CPS discusses and/or refers to some of those policies, procedures and documentation in order to provide a general overview of the QV-PKI and its operations.

1.3.1. QV-Providers

1.3.1.1. QV-RCA Functions

The functions performed by the QV-RCA include:

- generation of its own Keys;
- issuing a self signed Certificate;

- publication of its Certificate in the QuoVadis X.500 Directory services;
- publication of its Root CA Hash on the web site at:www.quovadis.bm;
- operation of the QV-RCA in an efficient and trustworthy manner;
- issuance of Certificates for QV Issuing CAs;
- publication of issued QV Issuing CA Certificates in the QuoVadis X.500 Directory services;
- investigation of compromises and suspected compromises of Private Keys at any level it deems warranted in its chain of trust;
- revocation of QV Issuing CA Certificates on receipt of authenticated digitally signed revocation requests, or when otherwise deemed warranted by the QV-RCA;
- posting revoked QV Issuing CA Certificates in the directory services CRL;
- conduct of regular internal security audits; and
- conduct of compliance audits of QV Issuing CAs when Certificate renewal is due.

1.3.1.2. QV Issuing CA Functions

QV Issuing CAs operating under the QuoVadis hierarchy perform the following functions:

- generate their own Keys;
- publish the QV-CP under which they issue Certificates, and any applicable CPS on a nominated web site;
- approve the naming conventions for the creation of distinguished names for Certificate applicants, in compliance with the X.520 standard for Distinguished Names;
- providing Authorised Relying Parties with access to:
  - Certificate information published in the directory services;
  - the public keys associated with Certificates that are listed in the directory services;
  - operate the QV Issuing CA in an efficient and trustworthy manner in accordance with the QV-CP and documented operational procedures;
- issue Certificates in accordance with the QV-CP and any contractual documentation to:
  - QuoVadis Registration Authorities (QV-RAs);
  - QuoVadis Registration Authority Operators (QV-RAOs);
  - QuoVadis Corporate Registration Authorities (QV-CRAs);
  - QuoVadis Corporate Registration Authority Operators (QV-CRAOs);
  - Responsible Persons within Sponsoring Organisations;
  - Users; and
  - Organisations, in connection with the Identification and Authentication of Devices;
- publish issued Certificates in a nominated X.500 Directory;
- investigate compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
- revoke Certificates on receipt of Authenticated digitally signed revocation requests, or when otherwise deemed warranted;
- post revoked Certificates in the Certificate Revocation List (CRL);
- conduct regular internal security audits;
- conduct compliance reviews of QV-Ras, QV-CRAs and Sponsoring Organisations when their respective Certificate renewal is due; and
- assist in audits conducted by or on behalf of the QV-RCA to validate the renewal of their own Certificates.

1.3.1.3. QV-RA Functions

QV-RAs perform the following functions:

- generate their own Keys;

- submit their Public Keys together with digitally signed Certification Requests to their superior QV-Issuing CA;
- operate in an efficient and trustworthy manner and in accordance with:
  - a QV-RA agreement (note that a QV-RA agreement, which is a contractual document, does not exist between QV Issuing CAs and QV-RAs that are the same legal entity, for example, the QV-CA and QV-RA);
  - the QV-CP;
  - its internal security and privacy policies;
  - documented operational procedures;
- register Subscribers including:
  - processing Certificate application information and documentation;
  - proposing and approving distinguished names for Applicants;
  - confirming that an Applicant's name does not appear in their list of compromised Subscribers;
  - generating Key Pairs for Applicants, or accepting Applicant generated Keys provided the Applicant can both prove possession of and establish their right to use the Key Pairs;
- submit Applicant Public Keys together with digitally signed Certification requests to their QV Issuing CA;
- seek to ensure that Private Keys and Certificates are not obtained by third parties prior to being received by the Applicant;
- process requests from Subscribers for the renewal or revocation of their Certificates, and generate digitally signed renewal or revocation requests to their QV Issuing CA;
-
- investigate compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
- initiate Certificate revocation when required;
- maintain a list of compromised Keys and compromised users and provide these lists to their superior QV-Issuing CA; and
- assist their QV Issuing CA with their compliance reviews to validate the renewal of their own Certificates.

1.3.1.4. QV-CRA Functions

QV-CRAs perform the following functions:

- generate their own Keys;
- submit their Public Keys together with digitally signed Certification Requests to their superior QV-Issuing CA;
- operate in an efficient and trustworthy manner and in accordance with:
  - a QV-CRA Agreement;
  - the QV-CP;
  - its internal security and privacy policies;
  - documented operational procedures;
- register Subscribers including:
  - processing Certificate application information and documentation;
  - proposing and approving distinguished names for Applicants;
  - confirming that an Applicant's name does not appear in their list of compromised Subscribers;
  - generating Key Pairs for Applicants, or accepting Applicant generated Keys provided the Applicant can both prove possession of and establish their right to use the Key Pairs;
- submit Applicant Public Keys together with digitally signed Certification requests to their QV Issuing CA;
- seek to ensure that Private Keys and Certificates are not obtained by third parties prior to being received by the Applicant;

- process requests from Subscribers for the renewal or revocation of their Certificates, and generate digitally signed renewal or revocation requests to their QV Issuing CA;
- investigate compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
- initiate Certificate revocation when required;
- maintain a list of compromised Keys and compromised users and provide these lists to their superior QV-Issuing CA; and
- assist their QV Issuing CA with their compliance reviews to validate the renewal of their own Certificates.

1.3.1.5. Sponsoring Organisation Functions

Sponsoring Organisations perform the following functions:

- nominate a person (and their replacement(s), from time to time) within their Organisation to act in accordance with and ensure compliance by the Sponsoring Organisation with its obligations within the QV-PKI;
- operate in an efficient and trustworthy manner and in accordance with:
  - a Sponsoring Organisation Agreement;
  - the QV-CP; and
  - any documented operational procedures.
- request the issue of Certificates by its QV Issuing CA following completion of its obligations with respect to the processing of those Certificate applications;
- request Certificate revocation when required; and
- assist their QV Issuing CA with their compliance reviews to validate their continued designation as a Sponsoring Organisation.

1.3.2. 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. Subscribers are not automatically Authorised Relying Parties unless specifically authorised by contract so to act.

Users should perform the following functions:

- request the issue, renewal and if appropriate, revocation of their Certificates;
- comply fully with their respective Certificate application process including, without limitation, the provision of all required information and documentation;
- review any Certificate issued to them and ensure the correctness of all information set out therein;
- secure their Private Key
- generate Key Pairs where the keys associated with a Certificate request are generated by the Subscriber; and
- use their Keys and Certificates in a manner and for a purpose consistent with the requirements of the QV-CP and their relevant User Agreements.

1.3.3. 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 the QV- CP and a Relying Party Agreement. Subscribers are not automatically Authorised Relying Parties. An Authorised Relying Party shall not place reliance on a Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance (as set out in the QV-CP)

and that Authorised Relying Party is otherwise in compliance with the terms and conditions of its Relying Party Agreement.

1.4. Applicability

Certificates supported within the QV-PKI are used to support secure electronic commerce and the secure exchange of information by electronic means and may be employed for the following general uses:

- Identification;
- Authentication;
- Providing data confidentiality; and
- Providing data integrity.

The uses for which a Certificate are suitable, restricted or prohibited are set out in the QV-CP and related User Agreement to which that Certificate relates.

1.5. Contact Details

This CPS is administered by the PMA.
Enquiries or other communications about this CPS should be addressed to QuoVadis Limited.

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 outlines the obligations of the QV-RCA, QV Issuing CAs, QV-RAs, QV-CRAs, Sponsoring Organisations, Subscribers and Authorised Relying Parties.

2.1.1. QV-RCA Obligations

QuoVadis discharges its obligations by:

- providing the operational infrastructure and certification services, including X.500 Directory and service provider software;
- making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit QuoVadis to operating in compliance with:
  - documented operational procedures; and
  - within applicable law and regulation;
- approving the establishment of all QV Issuing CAs and on approval, executing a QV Issuing CA Agreement (save in respect of the QV-CA);
- maintaining this CPS and enforcing the practices described within it and in all relevant collateral documentation;
- publishing its Root CA Hash on the www.quovadis.bm web site and other nominated web sites;
- issuing QV Issuing CA Certificates to QV Issuing CAs, that comply with X.509 standards and are suitable for the purpose required;

- issuing QV Issuing CA Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
- publishing issued QV Issuing CA Certificates without alteration in the X.500 Directory;
- investigating any suspected compromise which may threaten the integrity of the QV-PKI;
- revoking QV Issuing CA Certificates in terms of section 4.4.1 - *Circumstances for revocation* and post such revoked Certificates in the X.500 Directory CRL;
- promptly notifying QV Issuing CA Certificate owners in the event it initiates revocation of their QV Issuing CA Certificates; and
- conducting compliance audits of QV Issuing CAs when their QV Issuing CA Certificate renewal is due.

2.1.2. QV Issuing CA Obligations

QV Issuing CAs in performing their functions will operate their certification services in accordance with:

- any QV Issuing CA Agreement;
- all Certificate Policies under which they issue Certificates (including the QV-CP);
- documented operational procedures; and
- applicable law and regulation.

2.1.3. QV-RA Obligations

QV-RAs discharge their obligations in accordance with the practices outlined in overview in this CPS, any applicable Certificate Policy (including the QV-CP) a QV-RA Agreement and all applicable documentation.

2.1.4. QV-CRA Obligations

QV-CRAs discharge their obligations in accordance with the practices outlined in overview in this CPS, any applicable Certificate Policy (including the QV-CP) a QV-CRA Agreement and all applicable documentation.

2.1.5. Sponsoring Organisation Obligations

Sponsoring Organisations discharge their obligations in accordance with the practices outlined in overview in this CPS, any applicable Certificate Policy (including the QV-CP) a Sponsoring Organisations Agreement and all applicable documentation.

2.1.6. Subscriber Obligations

Subscribers are required to act in accordance with any applicable Certificate Policy (including the QV-CP) and their relevant User Agreement and all applicable documentation.

2.1.7. Authorised Relying Party Obligations

Authorised Relying parties are required to act in accordance with any applicable Certificate Policy (including the QV-CP) and their relevant Relying Party Agreement and all applicable documentation

2.2. Liability

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

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

These measures include but are not limited to:

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

2.2.1. QuoVadis Liability

Limitations upon and the extent of the liability of QuoVadis, QV Issuing CAs, QV-CRAs and Users may vary and are described within the QV-CP and relevant contractual documents.

2.2.2. Financial Responsibility

2.2.2.1. Indemnification Provisions

Indemnity provisions and obligations are contained within relevant contractual documentation.

2.2.2.2. Fiduciary Relationships

Issuing Certificates, or assisting in the issue of Certificates does not make a QV Provider an agent, fiduciary, trustee, or other representative of Users.

2.2.3. Administrative Processes

Administrative processes are dealt with and described in detail in the various documents used within and supporting the QV-PKI.

2.2.4. Maintenance of Financial Records

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

2.2.5. Insurance

QuoVadis maintains in full force and effect an errors and omissions insurance policy.

2.2.6. Demonstration of Financial Responsibility

QV Issuing CAs are required to demonstrate financial responsibility as referred to in the relevant QV Issuing CA Agreement.

2.3. Interpretation and Enforcement

2.3.1.1. Governing Law

This CPS i is governed by the laws of Bermuda without reference to conflicts of law principles.

2.3.1.2. Notice

A notice, consent, request or any other communication required under the practices described or referred to in this CPS shall be in the form of and otherwise be required to comply with the relevant contractual agreement.

2.4. Fees

2.4.1. Certificate Issuance or Renewal Fees

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

2.4.2. Certificate Access Fees

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

2.4.3. Revocation or Status Information Access Fees

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

2.4.4. Fees for Other Services

No fee is to be levied for access to the QV-CP or this CPS via the Internet. A fee may be charged by a QV Issuing CA for printed copies of this QV-CP or the CPS. Printed copies of this CPS are available from QuoVadis for a fee determined by QuoVadis, from time to time, plus postage and handling.

2.4.5. Refund Policy

QuoVadis or QV Issuing CAs under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements.

2.5. Publication and Repository

2.5.1. Publication of QV-RCA Information

Access to QuoVadis documentation is generally controlled and restricted to persons participating in the QV-PKI.

2.5.1.1. Electronic Publication

This CPS is published electronically in PDF format at www.quovadis.bm/

2.5.1.2. Hard Copy Publication

Paper copies of this CPS are available to persons entitled thereto from QuoVadis for a fee.

2.5.1.3. Publication by CAs

Issues as to publication of documentation by QV Issuing CAs are dealt with in relevant QV Issuing CA contractual documentation.

2.5.2. Frequency of Publication

Certificates are published promptly following their generation and issue. CRL publication is in accordance with section 4.4.9 *CRL Issuance Frequency*. Newly approved versions of this CPS, Certificate Policies (including the QV-CP), User Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions of those agreements.

2.5.3. Access Controls

QuoVadis does operate access controls in connection with the availability of documentation. Access is generally available only to participants in the QV-PKI where deemed necessary.

2.5.4. Repositories

The Repository for QuoVadis is provided by the QV-PKI applications.

2.5.4.1. X.500 Directory Functions

The X.500 Directory provides Certificate information services.

2.5.4.2. X.500 Directory Availability

QuoVadis seeks to provide availability for the X.500 Directory 7 days a week, 24 hours a day, subject to routine maintenance.

2.5.4.3. Restrictions on X.500 Directory Access and Services

Access to Certificate information is limited and set out within the relevant contractual documents.

2.5.4.4. Repository Publication

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

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-CPS, and other related operational policies and procedures

2.6.1.1. Identity/Qualifications of Auditor

The audit services described in Section 2.6.1 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. 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

2.7.1. Types of Information to be Kept Confidential

2.7.1.1. Collection and Use of Personal Information

Information supplied to QuoVadis as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines.

Access to confidential information by operational staff is on a need-to-know basis.
The QuoVadis System Security Policy (QV-SSP) contains details regarding the treatment of confidential information.

2.7.1.2. Registration Information

All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or rejected;
- POI documentation and details;
- Certificate information collected as part of the registration records, but this does not act to prevent publication of Certificate information in the X.500 Directory;
- User Agreements;
- any information requested by QuoVadis when it receives an application from a third party to operate a QV Issuing CA.

2.7.1.3. Certificate Information

The reason for a Certificate being revoked is considered to be confidential information, with the sole exception of the revocation of a QV-Provider's Certificate due to:

- the compromise of their Private Key, in which case a disclosure may be made that the Private Key has been compromised;
- the termination of the QV Provider, in which case prior disclosure of the termination may be given.

2.7.1.4. QV-Provider Documentation

The following QV-Provider documents are considered to be confidential:

- Concept of Operations;
- QV Issuing CA and/or RA Agreement;
- QV-RA Agreement;
- QV-CRA Agreement;
- Sponsoring Organisation Agreement;
- Protective Security Risk Review;
- System Security Plan;
- Contingency & Disaster Recovery Plan;
- Configuration Baseline; and
- Operating Procedures.

2.7.2. Types of Information not Considered Confidential

2.7.2.1. Certificate Information

Certificates published in the X.500 Directory are not considered to be confidential information.

2.7.2.2. QV-Provider Documentation

The following QV-Provider documents are public documents and are not considered to be confidential information (i.e. available to participants within the QV-PKI):

- the QV-CP;
- this CPS; and

- Privacy Policy (Public).

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

2.8.1. General

QuoVadis is in possession of, or holds licences for the use of hardware and software in support of the QV-PKI as outlined in this CPS. The use of the PKIX IETF Draft 4 Guideline is acknowledged. QuoVadis excludes all liability for breach of any other intellectual property rights.

2.8.1.1. QuoVadis

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.

2.8.1.2. Public and Private Keys

If the Subscriber generates the Public and Private Key Pair to the satisfaction of the QV Issuing CA then the Subscriber grants to the QV Issuing CA the right to publish and propagate in the QV Issuing CA Directory the Public Key that corresponds to the Private Key that is in the possession of the Subscriber. This publication will be through the incorporation of the Public Key in the Certificate (whether electronic or otherwise) that forms part of the QV Issuing CA Directory. Nothing in this clause grants to the Subscriber any rights whatsoever in relation to the format or structure of the Certificate that encompasses the Subscriber Public Key.

If a QV-RA generates the Subscriber Public and Private Key Pair then the QV-RA assigns to the Subscriber all intellectual property including copyright (if any) in the Private Key but not the Public Key. The QV-RA grants to the QV Issuing CA the right to publish and propagate in the QV Issuing CA Directory the Public Key that corresponds to the Private Key that is in the possession of the Subscriber. This publication will be through the incorporation of the Public Key in the Certificate (whether electronic or otherwise) that forms part of the QV Issuing CA Directory. Nothing in this clause grants to the QV-RA or the Subscriber any rights whatsoever in relation to the format or structure of the Certificate that encompasses the Subscriber Public Key

2.8.1.3. Certificate

QuoVadis reserves the right at any time a revoke any Certificate in accordance with the procedures and policies set out in the QV-CP or contractual documentation relevant to that Certificate.

2.8.1.4. Distinguished Names

Intellectual property rights in distinguished names vest in QuoVadis unless otherwise specified in the QV-CP, contract or other agreement, e.g. User Agreement.

2.8.2. Copyright

The intellectual property in this CPS is the exclusive property of QuoVadis.

2.8.2.1. OID

Copyright in the Object Identifiers (OID) for the QuoVadis infrastructure vest solely in QuoVadis.

OIDs are not to be copied, used or otherwise dealt with in any way except as provided for in the operation of the QuoVadis infrastructure, or in accordance with the QV-CP or this CPS.

3. Identification and Authentication

3.1. CA and RA Initial Registration

A fundamental concept underpinning the operation of the QV-PKI is trust. Trust must be realised in each and every aspect of the service operation. At QuoVadis' discretion, other trustworthy parties may be permitted to operate QV Issuing CA, QV-RA, QV-CRA and Sponsoring Organisation services within the QV-PKI.

QuoVadis seeks to ensure the integrity of the QV-PKI operational hierarchy through contractual agreements with QV Issuing CAs QV-RAs, QV-CRAs and Sponsoring Organisations following their acceptance by QuoVadis as a QV Issuing CA, QV-RA, QV-CRA or Sponsoring Organisation pursuant to a formal application procedures. QuoVadis does not permit private individuals to operate QV Issuing CA QV-RA, QV-CRA and Sponsoring Organisation services within the QV-PKI.

3.2. Requirements for commencement of operations

If the application to operate QV Issuing CA, QV-RA, QV-CRA or Sponsoring Organisation services is approved, prior to commencement of operations:

- QuoVadis advises the new service provider of its OID (if applicable) and distinguished name;
- QuoVadis advises the QV Issuing CA, QV-RA, QV-CRA or Sponsoring Organisation of the required software and hardware (if any);
- the new QV Issuing CA, QV-RA, QV-CRA or Sponsoring Organisation establishes under QuoVadis' auspices, a range of policy, planning and operational documentation; and
- all operational procedures are vetted for compliance before they are implemented.

3.3. Initial registration

3.3.1. Types of names

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

The QV-RCA approves naming conventions for the creation of distinguished names for QV Issuing CAapplicants. Different naming conventions may be used in different policy domains.

QV-RAs and QV-CRAs propose and approve distinguished names for Applicants, and as a minimum check that a proposed distinguished name is unique, verify that the name is not already listed in the QuoVadis X.500 Directory.

3.3.2. Need for names to be meaningful

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

3.3.3. Recognition, authentication and role of trademarks

This is a commercial issue and as such is dealt with by relevant contractual documents.

3.3.4. Method to prove possession of Private Key

Where Key Pairs are generated by an Applicant, the relevant QV-Provider must satisfy themselves that the Applicant does in fact possess the Private Key that correspond to the Public Key received from the Applicant. This may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the Applicant.

The relevant QV Provider is to also take reasonable steps to ensure the Applicant is the true owner of the Key Pairs. Reasonable steps might typically consist of:

- the relevant QV Provider checking, and arranging for any other QV Providers within the policy domain to check, their records to ensure the Public Keys are not already listed against any current operational or revoked Certificate; and
- if deemed appropriate, obtaining a statutory declaration from the Applicant that they are the true owner of the Key Pairs.

If any doubt exists, the relevant QV Provider should not to perform certification of the Key.

3.3.5. Authentication of Organisation identity

An Organisation's Identity is to be Authenticated in accordance with all relevant application and other documentation.

3.3.6. Authentication of Individual identity

An Individual's Identity is to be Authenticated in accordance with all relevant application and other documentation.

3.4. Routine Rekey

QuoVadis does not support routine rekey. Key Pairs must always expire at the same time as the associated Certificate. If a renewal request is accepted, both new Certificates and new Key Pairs are issued.

3.5. Rekey after Revocation

Rekey is not permitted after Certificate revocation. Application for a Certificate following revocation is treated as though the person requesting renewal were a new Applicant.

3.6. Revocation request

A request to revoke Keys and Certificates may be submitted by persons authorised to do so under relevant contractual documentation including the QV-CP.

4. Operational Requirements

4.1. Certificate Application

Certificate applications are subject to various assessment procedures depending upon the type of Certificate applied for and the intended status of the Certificate within the QV-PKI. Certificate applications from persons wishing to act as QV Issuing CAs are dealt with direct by the QV-RCA and the requirements associated therewith are set out in the relevant documents dealing with application for approval as a QV Issuing CA. Certificate application requirements from Subscribers are set out and dealt with in the relevant application forms governing the type of Certificate applied for.

4.2. Certificate issuance

Certificate issuance is governed by and should comply with the practices described in and any requirements imposed by the QV-CP.

4.3. Certificate Acceptance

Certificate acceptance is governed by and should comply with the practices described in and any requirements imposed by the QV-CP and any other relevant agreement under which the Certificate is being issued.

4.4. Certificate Revocation

4.4.1. Circumstances for revocation

Revocation can be described as no longer being able to use a Certificate. Certificate revocation is governed by and should comply with the practices described in and any requirements imposed by the QV-CP and any other relevant agreement under which the Certificate was issued.

4.4.2. Who can request revocation

Certificate revocation, including details as to persons authorised to request revocation, is governed by and should comply with the practices described in and any requirements imposed by the QV-CP and any other relevant agreement under which the Certificate was issued.

4.4.3. Procedure for revocation request

The practices involved in processing of a revocation request will vary depending on the identity of the originator and are governed by and should comply with the practices described in and any requirements imposed by the QV-CP and any other relevant agreement under which the Certificate was issued.

4.4.4. Revocation request grace period

No grace period is permitted once a revocation request has been verified.

4.4.5. Circumstances for suspension

No suspension of Certificates is permissible within the QV-PKI.

4.4.6. Who can request suspension

No suspension of Certificates is permissible within the QV-PKI.

4.4.7. Procedure for suspension request

No suspension of Certificates is permissible within the QV-PKI.

4.4.8. Limits on suspension period

No suspension of Certificates is permissible within the QV-PKI.

4.4.9. CRL issuance frequency

The CRL in the X.500 Directory is updated at the time of Certificate revocation.

4.4.10. 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:

- 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.
- 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.

4.4.11. 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.

4.4.12. Other forms of revocation publication available

Although there is no requirement to do so, QV Issuing CAs may use additional methods to publicise Certificate revocation.

4.4.13. Checking requirements for other forms of revocation advertisements

No requirement.

4.4.14. Special requirements re Key compromise

There are no variations to the above Certificate revocation and suspension procedures when the revocation or suspension is due to Private Key Compromise.

4.5. Security Audit procedures

Security Audit procedures as set out in the QV-Security and Audit Procedures Document (QV-SAP) apply to the QV-PKI and the participants therein including the QV-RCA, QV Issuing CAs, QV-RAs and QV-CRAs.

4.5.1. Types of event recorded

The minimum audit records to be kept are detailed in the QV-SAP.

4.5.2. Frequency of processing log

Audit logs are required to be processed in accordance with QV-SAP.

4.5.3. Retention period for audit log

Audit logs should be retained in accordance with the QV-SAP.

4.5.4. Protection of audit log

Audit logs are encrypted in accordance with the QV-SAP.

4.5.5. Audit log backup procedures

Each service provider in the QuoVadis hierarchy should establish and maintain a backup procedure for audit logs in accordance with the QV-SAP.

4.5.6. Audit collection system

The QuoVadis audit collection system is detailed in the QV-SAP.

4.5.7. Notification to event-causing subject

There is no requirement to notify the event causing subject that an event was audited.

4.5.8. Vulnerability assessments

Individual threat and risk assessments are required at each level of the QV-PKI including QV issuing CAs.

4.6. Records Archival

Each service providers in the QuoVadis hierarchy maintains an archive of relevant records as required by relevant contractual documentation.

4.6.1. Types of event recorded

Audit information required to be recorded and archived by service providers is detailed in the QV-SAP.

4.6.2. Retention period for archive

Requirements as to archiving are dealt with in the QV-CP and other relevant agreements.

4.6.3. Protection of archive

Archive media is protected either by physical security, or a combination of physical security and cryptographic protection as set out in the QV-CP and other relevant agreements.

4.6.4. Archive backup procedures

Each QV Provider should establish archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster situation as detailed in the QV-CP and relevant operational agreements.

4.6.5. Requirements for time-stamping of records

Trusted third party time stamping is supported and is set out in the QV-CP and relevant operational agreements.

4.6.6. Archive collection system

Each QV Provider should establish an archive collection system in accordance with the relevant QV Issuing CA Operating Policies and Procedures.

4.6.7. Procedures to obtain and verify archive information

The integrity of a QV Provider's archives are to be verified in accordance with the QV Issuing CA Operating Policies and Procedures.

4.7. Key changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates and, with the exception of the QV-RCA which issues a new Certificate and new Keys to itself, all

parties within the QV-PKI are to obtain new keys by making an application for Certificate renewal in accordance with the QV-CP and relevant contractual documentation.

4.8. Compromise and Disaster Recovery

QuoVadis has established a CA Operations Disaster & Recovery Plan (QV-BCP). The purpose of this plan is to restore core business operations as quickly as practicable when systems operations have been significantly and adversely impacted by fire, strikes, etc.

The plan acknowledges that any impact on system operations will not cause a direct and immediate operational impact within the QV-PKI of which the service provider is a part. The primary goal of the plan is to reinstate the service provider platform in order to make accessible the logical records kept within the software.

4.8.1. Computing resources, software, and/or data are corrupted

The establishment of a configuration baseline plan, and back-up, archiving and response plan to provide data for identifying component failure and subsequent service restoration is dealt with in the QV-BCP.

4.8.2. Entity Public Key is revoked

The establishment of a Key and User compromise plan that addresses the actions to be taken in the event that the QV-RCA or QV Issuing CA Public Key is revoked is dealt with in the QV-BCP.

4.8.3. Entity Key is compromised

The establishment of a Key and User compromise plan that addresses the actions to be taken in the event that a Private Key is compromised is dealt with in the QV-BCP.

4.8.4. Secure facility after a natural or other type of disaster

Each QV Provider is required to manage its backup, archive and offsite storage in accordance with the QV-BCP.

4.9. QV Issuing CA Termination

When it is necessary to terminate a QV Issuing CA service, the impact of the termination is to be minimised as much as possible in light of the prevailing circumstances and is subject to the QV Issuing CA Agreement.

4.9.1. Notice

Notice requirements are set out in the relevant QV Issuing CA Agreement.

4.9.2. User Keys and Certificates

Where practical, Key and Certificate revocation should be timed to coincide with the progressive and planned rollout of new Keys and Certificates by a successor QV Issuing CA.
Compensation or restitution to Users for the revocation of their Certificates prior to their expiry date that falls outside the scope of this CPS.

4.9.3. Successor QV Issuing CA

To the extent that it is practical and reasonable the successor QV Issuing CA should assume the same rights, obligations and duties as the terminating QV Issuing CA. The successor QV Issuing CA should issue new Keys and Certificates to all subordinate service providers and Users whose Keys and Certificates were revoked by the terminating QV Issuing CA due to its termination, subject to the individual service provider or User making an application for a new Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or User Agreement.

5. Physical, Procedural And Personnel Security Controls

5.1. Physical Controls

The provisions in this section are applicable only to the QV-RCA and the QV-CA. Physical, procedural and personnel controls for QV Issuing CAs and QV-RAs (other than the QV-CA) are specified in the relevant QV Issuing CA Operating Policies & Procedures.

5.1.1. Site location and construction

The site location of QuoVadis is in a secure office environment in Bermuda. QuoVadis operates within a secure physical environment within the office area that meets the standards of an independent security certification body, at a highly protected level.

5.1.2. Physical access

QuoVadis permits entry to its secure operating area only to authorized personnel in accordance with its Operating Policies & Procedures (QV-OPP).

5.1.3. Power and air conditioning

The QuoVadis secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

5.1.4. Water exposures

The QuoVadis secure operating area provides protection against water.

5.1.5. Fire prevention and protection

The QuoVadis secure operating area provides protection against fire.

5.1.6. Media storage

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

5.1.7. Waste disposal

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

- in the case of magnetic media:
  - physical damage to, or complete destruction of the asset;
  - the use of an approved utility to wipe or overwrite magnetic media;
- in the case of printed material, shredding, or destruction by an approved service.

5.1.8. Off-site backup

Endorsed off site storage agents are used for the storage and retention of backup software and data.
The off site storage:

- is available to authorized personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and
- has appropriate levels of physical security in place.

5.2. Procedural Controls

5.2.1. Trusted roles

In order to ensure that one person acting alone cannot circumvent the entire system, responsibilities are shared by multiple roles and individuals. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. At a minimum, the following roles are established:

- System Administrator;
- Registrar (RAs only); and
- Security Administrator.

5.2.2. Number of persons required per task

Separate individuals fill each of the three roles described above in accordance with the QV-OPP.

5.2.3. Identification and authentication for each role

Persons filling trusted roles must undergo an appropriate security screening procedure, designated “Position of Trust” as set out in the QV-OPP.

5.3. Personnel Controls

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

All Key Pairs should be generated in a secure manner as set out in the relevant CA Operations, Policies and Procedures document.

6.1.2. Private key delivery to entity

Delivery of Keys is dealt with in the relevant CA Operations, Policies and Procedures documentation.

6.1.3. Public key delivery to certificate issuer

Delivery of Keys is dealt with in the relevant CA Operations, Policies and Procedures documentation.

6.1.4. CA public key delivery to users

Delivery of Keys is dealt with in the relevant CA Operations, Policies and Procedures documentation.

6.1.5. Key sizes

Key lengths within the QV-PKI are determined by Certificate profiles and are detailed in the QV-CP.

6.1.6. Public Key parameters generation

The parameters used to create Public Keys are generated by the relevant QV Provider application, except for self-generated User keys in which case the parameters are generated by the User's client application.

6.1.7. Parameter quality checking

The quality of Public Key parameters is automatically checked by the QV Provider application that generates the Key, except for self-generated User Keys in which case the parameters are quality checked by the QV-RA or QV-CRA prior to submitting a certification request to the QV Issuing CA.

6.1.8. Hardware/software key generation

QV Provider and Subscriber Key generation may be performed in hardware or software.

6.1.9. Key usage purposes

Keys may be used for the purposes and in the manner described in the QV-CP.

6.2. Private Key Protection

6.2.1. Standards for cryptomodule

Cryptomodules in use within QuoVadis comply with industry standards.

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

QV Issuing CA Private Keys are stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secure off site storage.

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

6.2.5. Private key 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 cryptomodule

If a cryptomodule is used, the Private Key must be generated in it and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which it is being used.

6.2.7. Method of activating Private Key

Private keys are activated in accordance with the QV-CP.

6.2.8. Method of deactivating Private Key

Private Keys are de-activated in accordance with the policies and procedures set out in the QV-CP.

6.2.9. Method of destroying Private Key

The methods of destroying Private Keys are set out in the QV-CP.

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 the Public and Private Keys

As prescribed within the QV-CP.

6.4. Activation Data

6.4.1. Activation data generation and installation

No activation data other than access control mechanisms is required to operate cryptomodules.

An User Personal Identification Code (PIC) may be generated by an RA during key pair creation, to protect the transport of an User's Keys and Certificates to the User.

6.4.2. Activation data protection

No activation data other than access control mechanisms is required to operate cryptomodules. PICs may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third party interception of the PIC.

6.4.3. Other aspects of activation data

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

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

QuoVadis has established an approved System Security Policy that incorporates computer security technical requirements that are specific to that Service Provider's operations.

6.5.2. Computer security rating

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

6.6. Life Cycle Technical Controls

6.6.1. System development controls

QV Provider and User client applications are developed in controlled environments employing appropriate quality controls.

6.6.2. Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1 *Trusted roles*.

6.6.3. Life cycle security ratings

QuoVadis has established an approved System Security Policy that identifies and addresses all high or significant life cycle security threats.

6.6.4. Network Security Controls

QuoVadis has established an approved System Security Policy that identifies and addresses all high or significant network security threats.

6.6.5. Hardware Cryptomodule Engineering Controls

QuoVadis has established an approved System Security Policy that identifies and addresses all high or significant cryptographic module engineering security threats.

7. Certificate and CRL Profiles

7.1. Certificate Profiles

The Certificate profile information contained in this section relates primarily to the QV-RCA and QV Issuing CA Certificates. The Certificate profile for end entity Certificates is described in the QV-CP.

7.1.1. Version number(s)

QuoVadis supports and uses Certificates as more particularly described in the Certificate Profiles.

7.1.2. Certificate extensions

As more particularly described in the Certificate Profiles.

7.1.3. Algorithm object identifiers

As more particularly described in the Certificate Profiles.

7.1.4. Name forms

As more particularly described in the Certificate Profiles.

7.1.5. Name constraints

Any applicable name constraints are set out in the QV-CP.

7.1.6. Certificate Policy Object Identifier

As more particularly described in the Certificate Profiles.

7.1.7. Usage of Policy Constraints extension

As more particularly described in the Certificate Profiles.

7.1.8. Policy qualifiers syntax and semantics

As more particularly described in the Certificate Profiles.

7.1.9. Processing semantics for the critical certificate policy extension

As more particularly described in the Certificate Profiles.

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 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 two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2. CRL and CRL Entry Extension

All User PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The applicable CPS or other publicly available document will identify and must define the use of any extensions supported by QV Issuing CAs, its QV-RAs and Users.

8. Specification Administration

QuoVadis operates the PMA that is responsible for setting Certificate policy direction for the overall public key infrastructure.
The QV-CP used under the QuoVadis hierarchy has been allocated an OID which:

- provides a unique identification for the CP; and
- includes a policy version number.

8.1. Specification change procedures

The PMA is the responsible authority for changes to the QV-CP and this CPS.

8.1.1. Change

There are two possible types of policy change:

- the issue of a new CP; and
- a change to or alteration of an existing policy.

If an existing policy requires re-issue, the change process employed is the same as for as for initial publication, as described above. Note that the new OID issued for a policy change differs from the previous OID only in the policy version number.

8.2. Publication and notification policies

New or amended CP are published on the web site nominated in the CP.
QV Issuing CAs are notified of changes to a CP as and when they are approved.

APPENDIX A

Definitions and Interpretation

In this QV-CPS 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).