1. Introduction 3
1.1. Overview ....

1. Introduction

1.1. Overview

The practices described in this Certification Practice Statement (CPS), together with the technologie

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 betwe

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 Q

- 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 r1254S3254 664.70.0j11384.0707 6684Certificate

- 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 Tm(S 0 10.91f-0.0

- 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

- 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 -

- 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

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, b

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
-

- 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.

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. Reasonabl

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 issue

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 accordan

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 an2 402.3543 413.1 Tm(e.c22.4601 Tm(the QV-CP an2 84m(4.6.3.)

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

5. Phys

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

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 acce

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 cons

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 ins

“**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 isA42.7797 Tm(that i)Tj1210.0302 403.8861 352 3a0

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**