1. Introduction

1.1. Overview

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: No independent Identification or Authentication required. Identity and related information is self-certified by the Applicant.

QV2 Certificate: In addition to self-certification by the Applicant, either (i) that Applicant's pre-existing relationship with the QV-RA, QV-CRA, or Sponsoring Organisation (or their respective Subsidiaries and Holding Companies) responsible for the Certificate application or (ii) with copies of documents supporting the claimed Identity of the Applicant are required. No Authentication of these documents is performed or required.

QV3 Certificate: In addition to self-certification by the Applicant, with either (i) 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 or (ii) certified true copies of documents that support the claimed Identity of the Applicant are required.

QV4 Certificate: In addition to self-certification by the Applicant, original documentation that supports the claimed Identity of the Applicant is required together with either (i) that 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 (ii) that Applicant's in person appearance before the relevant QV-RA.

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)

- 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 ef

- 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.

1.3.1.5ing CA; and

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 commer

- 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 function5109 630.2412 Tm(u)Th1m(m)Tj9.93596 630.2412 Tm(11.04 0 0 1m(f)Tj

- 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 pow

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

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

- Privacy Policy (Public).

2.7.3. Disclosure of Certificate Revocation Information

Certificate revocation information is provided via the CRL in the Q

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 (ty

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 s

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 aceq3 6t53207j.

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 requirement

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

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 reeline

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, Phy

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 9.96 0 0 9.96 4d28s 597.3609 Tm(ation 97m(h)Tj9.96 0 0 928007 Tm(pons)Tj9.96 0 0 9.96 424r)Tj9.96

6.1.5. Key sizes

Key lengths within the Q

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.

6.6.2. 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-RCA0 9.96 462.8339 460.96

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) c

“**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, signatur

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