CERTIFICATION PRACTICE STATEMENT - RCA

O.I.D: 1.3.6.1.4.1.8024.0.1.2000.1
Effective Date: August 1 st 2003
Version: 2.0 6

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 set forth herein.

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 ( )0.7 (ner)ompl 567 (ner)uruoV92

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.

- 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.

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 Informat ion 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. Repositortbp (s)]TJ 0 Tc 0 T6.03359 0 Td ( )Tj EMC /P <</MCI3 1 >>BDC /TT2 1 Tf -0.002 Tc 0

2.7. Confidentiality

2.7.1. Types of In formation 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;
-

- 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

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.ororttTJ 0 Tche us40 Tc9 (or)6.c

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 with9 (i)3.1-1.1 (or)-602d verbe 1 (de

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

-

5. Physical, Procedural And Personnel Security Controls

5.1. Physical C ontrols

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-OPermrrQTJ r3.2

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.

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

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.

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 (ii) who the Qv-RA, ga ng1Td (-)Tj 0.374 0

“

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