Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement herein after referred to as the CP/CPS adopted by QuoVadis Limited (QuoVadis). The QuoVadis CP/CPS contains an overview of the practices and procedures that QuoVadis employs for its operation as a Digital Certification 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 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 CP/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 CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

Contact Information:

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

Mailing Address:
QuoVadis Limited
Suite 1640
48 Par-La-Ville Road
Hamilton HM-11
Bermuda

Website: www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

Version Control:

Author	*Date*	*Version*	*Comment*
QuoVadis PMA	1 December 2006	1.0	Baseline for Root Ceremony
QuoVadis PMA	15 December 2006	1.5	Edits for EV compliance
QuoVadis PMA	28 December 2006	1.6	Formatting and corrections
QuoVadis PMA	12 January 2007	1.7	Corrections to cert policies
QuoVadis PMA	02 October 2007	1.8	Revisions for v1 of EV Guidelines
QuoVadis PMA	27 May 2008	1.9	Updated to reflect V1.1 of EV Guidelines
QuoVadis PMA	22 April 2010	1.10	Update for EV Guidelines Errata and

Table of Contents

1. INTRODUCTION

1.1. Overview

QuoVadis SSL Certificates are issued for use with the SSL 3.0/TLS 1.0 protocol to enable secure transactions of data through privacy, authentication, and data integrity.

QuoVadis Trusted Code Signing Certificates are used to provide users with reasonable assurance that the executable code they download comes from a source identified by QuoVadis.

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that QuoVadis Root CA2 uses in the generation, issue, use, and management

The diagram below illustrates the components of the QuoVadis PKI:

1.3.2. Registration Authorities

QuoVadis acts as Registration Authority (RA) for Certificates it issues. An RA is an entity that performs verification of Certificate Holder information in accordance with this CP/CPS, and revokes Certificates upon receipt of a valid request from an authorised person.

Third parties, who enter into a contractual relationship with QuoVadis, may act as Local Registration Authorities (LRAs) and authorise the issuance of Certificates by QuoVadis for Organisations and Domains that have been pre-authenticated by QuoVadis. LRAs must abide by all the requirements of this CP/CPS and the terms of their services agreement with QuoVadis. LRAs may also implement more restrictive practices based on their internal requirements.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using the QuoVadis Repository.

Repository: The Repository refers to the CRL, OCSP, and other directory services provided by QuoVadis containing issued and revoked Certificates.

Acronyms

CA	Certificate Authority or Certification Authority
CP/CPS	Certificate Policy & Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
PMA	QuoVadis Policy Management Authority
EV	Extended Validation
FIPS	Federal Information Processing Standard
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
LRA	Local Registration Authority
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSI TORY RESPONSIBILITIES

2.1. Repositories

The QuoVadis Repository serves as the primary repository for revocation data on issued Certificates. However, copies of QuoVadis directories may be published at such other locations as required for efficient operation of the QuoVadis PKI.

2.2. Publication of Certificate Information

QuoVadis operates and maintains its Repository with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the Certificates issued by its CAs.

QuoVadis publishes Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) resources to allow Relying Parties to determine the validity of a QuoVadis Certificate. Each CRL contains entries for all revoked un-expired Certificates issued. QuoVadis maintains revocation entries on its CRLs, or makes Certificate status information available via OCSP, until after the expiration date of the revoked Certificate.

2.3. Time or Frequency of Publication

QuoVadis issues a new CRL at least every twelve (12) hours and prior to the expiration of the current CRL. QuoVadis also provides an OCSP resource that is updated at least every twelve (12) hours. Certificate information is published promptly following generation and issue, and within 20 minutes of revocation.

2.4. Access Controls on Repositories

Participants (including Certificate Holders and Relying Parties) accessing the QuoVadis Repository and other QuoVadis directory resources are deemed to have agreed with the provisions of this CP/CPS and any other conditions of usage that QuoVadis may make available. Participants demonstrate acceptance of the conditions of usage of this CP/CPS by using a QuoVadis Certificate. Failure to comply with the conditions of usage of the QuoVadis Repository and web site may result in termination of the relationship between QuoVadis and the party, at QuoVadis' sole discretion, and any unauthorised reliance on a Certificate shall be at that party's risk. QuoVadis is the only entity that has write access to Repositories.

3. IDENTIFICATION AND AUTHENTICATION

The identification and authentication procedures used by QuoVadis depend on the class of Certificate being issued. See Appendix B for Certificate Profiles and the relevant verification requirements.

3.1. Naming

3.1.1. Types Of Names

All Certificate Holders require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). SSL Certificates are issued using the Fully Qualified Domain

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

Certificate issuance is governed by the practices described in and any requirements imposed by this CP/CPS.

4.3.2. Notification To Certificate Holder By The CA Of Issuance Of Certificate

Certificates are delivered to the Certificate Requester designated in the Certificate Application.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsible for installing the issued Certificate on the Certificate Holder's computer or cryptographic module according to the Certificate Holder's system specifications. A Certificate Holder is deemed to

Parties who are not the Certificate Holder (such as Relying Parties, Application Software Vendors, and other third parties) may file a Certificate Problem Report to initiate a Certificate revocation request. Problem reports may include complaints; suspected private key compromise or Certificate misuse; or other types of fraud, compromise, misuse, or inappropriate conduct related to the Certificate.

4.9.3. Procedure For Revocation Request

QuoVadis will revoke a Certificate upon receipt of a valid request from the Certificate Holder, verified through an out-of-band communication.

QuoVadis will begin an investigation of all Certificate Problem Reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;
(ii) Number of Certificate Problem Reports received about a particular Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

QuoVadis maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. QuoVadis will revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time Within Which The CA Must Process The Revocation Request

QuoVadis will take commercially reasonable steps to revoke the Digital Certificate within 4 hours of receipt of a valid revocation request.

4.9.6. Revocation Checking Requirement For Relying Parties

Relying Parties are required to consult the QuoVadis Repository of issued and revoked Certificates at all times prior to relying on information featured in a Certificate. Failure to do so negates the ability of the Relying Party to claim that it acted on a Certificate with reasonable reliance.

4.9.7. CRL Issuance Frequency

QuoVadis manages and makes publicly available directories of revoked Certificates through the use of CRLs. All CRLs issued by QuoVadis adhere to X.509v2 CRL as profiled in RFC 5280.

QuoVadis updates and publishes a new CRL of revoked Certificates on a 12-hour basis (or more frequently under special circumstances) and within 5 minutes of a Digital Certificate Revocation. The CRLs for Certificates issued pursuant to this CP/CPS can be accessed via the URLs contained in the Certificate Profile for that Certificate. The CRL is published and is available 24 hours a day, 7 days a week, and 52 weeks of the year every year

4.9.8. Maximum Latency For CRL

The maximum latency for the CRL is 10 minutes.

4.9.9. On-Line Revocation/Status Checking Availability

QuoVadis provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of the Certificate.

4.9.10. On-Line Revocation Checking Requirement

Relying Parties are required to consult the QuoVadis Repository of issued and revoked Certificates at all times prior to relying on information featured in a Certificate. Failure to do so negates the ability of the Relying Party to claim that it acted on a Certificate with reasonable reliance.

4.9.11. Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements for Key Compromise
QuoVadis will use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that a CA's private key has been compromised.

4.9.13. Circumstances For Suspension
The QuoVadis PKI does not supportsuspension of Certificates.

4.9.14. Who Can Request Suspension
The QuoVadis PKI does not supportsuspension of Certificates.

4.9.15. Procedure For Suspension Request
The QuoVadis PKI does not supportsuspension of Certificates.

4.9.16. Limits On Suspension Period
The QuoVadis PKI does not supportsuspension of Certificates.

4.10. Certificate Status Services
Not applicable.

4.11. End Of Subscription
A Certificate Holder may terminate its subscription to the QuoVadis PKI by allowing a Certificate or applicable agreement to expire without renewal, or by voluntarily revoking a Certificate.

4.12. Key Escrow And Recovery
The QuoVadis PKI does not support key escrow orrecovery of Certificate Holder private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
The section of the CP/CPS provides a high level descriptionof the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by QuoVadis to provide trustworthy and reliable CA operations.

5.1. Physical Controls
5.1.1. Site Location and Construction
QuoVadis performs its CA operations from a secure datacentre located in an office complex in Bermuda. The QuoVadis datacentre meets the standards of an independent security certification body at a highly protected level. Standards and protections include: certified BS-EN 1047 performance backed by ISO9000/1/2 liability insurance; fire (according to DIN 4102 F90) with an automatic FM200 extinguishing system; smoke and humidity (according to DIN 18095); burglary and vandalism (ET2 according to DIN 18103); and protection against electromagnetic influences and radiation (such as electromagnetic pulse).

5.1.2. Physical Access
QuoVadis permits entry to its secure operating area within the datacentre only to security cleared and authorised personnel, whose movements within the facility are logged and audited. Physical access is controlled by a combination of physical access cards and bnts wonce bL 0 TDTc .1ombi9ic FM200 e200c .1ombi0933 0 TD .0002 Tc .314 Tw [(ed and a

5.1.6. Media Storage

All magnetic media containing QuoVadis

For purposes of mitigating the risk that one individual acting alone could compromise the integrity of the QuoVadis PKI or any Certificate issued therein, QuoVadis performs relevant background checks of individuals and defines the tasks that the individuals will be responsible to perform. QuoVadis determines the nature and extent of any background checks in its sole discretion. The foregoing fully stipulates QuoVadis' obligations with respect to personnel controls and QuoVadis shall have no other duty or responsibility with respect to the foregoing. Without limitation, QuoVadis shall not be liable for employee conduct that is outside of their duties and for which QuoVadis has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.2. Background Check Procedures
Background check procedures include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Criminal records
- Credit/financial history and status
- Driving licenses
- Social security records

Where the above checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, QuoVadis will utilise available substitute investigation techniques permitted by law that provide similar information including background checks performed by applicable government agencies.

5.3.3. Training Requirements
QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities. This includes specific vetting training for Validation Specialists, who may not undertake Certificate validation and issuance until they have passed a suitable examination on knowledge and skills.

5.3.4. Retraining Frequency And Requirements
Validation Specialists engaged in Certificate validation and issuance must maintain adequate skill levels in order to have issuance privilege, consistent with QuoVadis' training and performance programs.

5.3.5. Job Rotation Frequency And Sequence
QuoVadis provides and maintains a program of job rotation in order to maintain appropriate and required levels of competency across key roles.

5.3.6. Sanctions For Unauthorised Actions
Appropriate disciplinary actions are taken for unauthorised actions.

5.3.7. Independent Contractor Requirements
The QuoVadis PKI does not support the use of independent contractors to fulfil roles of responsibility.

5.3.8. Documentation Supplied To Personnel
QuoVadis provides personnel all required training materials needed to perform their job function and their duties under the job rotation program. This includes specific documentation of the validation, issuance, and revocation processes for Certificates.

5.4. Audit Logging Procedures
5.4.1. Types Of Events Recorded
All events involved in the generation of the CA key pairs are recorded. This includes all configuration data used in the process.

Individuals who have access to particular key pairs and passwords will be audited. Key pair access will take the form of PIN-protected cryptographic smart cards. Access to the Oracle database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of

two people being present to perform certain tasks on QuoVadis CAs. The types of data recorded by QuoVadis include but are not limited to:

- All data involved in each individual Certificate registration process will be recorded for future reference if needed;
- All data and procedures involved in the certification and distribution of Certificates will be recorded, including records of verification checks;
- All data relevant to the publication of Certificates and CRL and OSCP entries will be recorded;
- All Certificate revocation request details are recorded including reason for revocation;
- Certificate and hardware security lifecycle management;
- Logs recording all network traffic to and from trusted machines are recorded and audited;
- All aspects of the configuration of the backup site are recorded. All procedures involved in the backup process are recorded;
- All data recorded as mentioned in the above sections is backed up. Therefore, there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios;
- All aspects of the installation of new or updated software;
- All aspects of hardware updates;
- All aspects of shutdowns and restarts;
- Time and date of log dumps;
- Time and date of transaction archive dumps; and
- Security profile changes

All audit logs will be appropriately time stamped and their integrity protected.

5.4.2. Frequency Of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3. Retention Period For Audit Log

Audit logs are retained as archive records for a period no less than eleven (11) years for audit trail files and for key and Certificate information. Audit logs are stored until at least eleven (11) years after the QuoVadis Issuing CA ceases operation.

5.4.4. Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI. Only CA Officers and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction. All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures

Each Issuing CA performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing CA premises and storage at a secure, offsite location.

5.4.6. Audit Collection System

The security audit process of each Issuing CA runs independently of the Issuing CA software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7. Notification To Event-Causing Subject

Where an event is logged, no notice is required to be given to the individual, organisation, device, or application that caused the event.

5.4.8. Vulnerability Assessment

Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the QuoVadis PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Issuing CA. Vulnerability assessment procedures intend to identify QuoVadis PKI threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders.

5.5. Records Archival

5.5.1. Types Of Records Archived

QuoVadis archives and makes available upon authorised request documentation subject to the QuoVadis Document Access Policy. For each Certificate, the records will address creation, issuance, use, revocation, expiration, and renewal activities. These records will include all relevant evidence in the Issuing CA's possession including:

- Audit logs;
- Certificate Requests and all related actions;
- Evidence produced in verification of Applicant details;
- Contents of issued Certificates;
- Evidence of Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- CRL lists posted; and
- Audit Opinions as discussed in this QuoVadis CP/CPS.

5.5.2. Retention Period For Archive

QuoVadis Issuing CA archives will be retained for a period of eleven (11) years.

5.5.3. Protection Of Archive

Archives shall be retained and protected against modification or destruction.

5.5.4. Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5. Requirements For Time-Stamping Of Records

QuoVadis supports time stamping of all of its records. All events that are recorded within the QuoVadis service include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis PKI rely on a trusted time source.

5.5.6. Archive Collection System

The QuoVadis Archive Collection System is internal.

5.5.7. Procedures To Obtain And Verify Archive Information

Only Issuing CA officers and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their authorised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.6. Key Changeover

Key changeover is not automatic but procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA private key's lifetime, QuoVadis ceases using its expiring CA private key to sign Certificates (well in advance of expiration) and uses the old private key only to sign CRLs associated with that key. A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active.

5.7. Compromise And Disaster Recovery

QuoVadis has a CA Operations Disaster & Recovery Plan (QuoVadis Business Continuity Plan). The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by fire, strikes, or other crisis events.

QuoVadis has in place business resumption procedures that provide for the immediate continuation of Certificate revocation services in the event of an unexpected emergency. QuoVadis regards its disaster recovery and business resumption plan as proprietary and it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.

QuoVadis has in place an appropriate key compromise plan detailing its activities in the event of a compromise of an Issuing CA private key. This plan includes procedures for:

- Revoking all Certificates signed with that Issuing CA's private key;
- Promptly notifying all Certificate Holders with Certificates issued by that Issuing CA; and
- Generating a new key pair and signing a new CA Certificate.

5.7.1. QuoVadis Business Continuity Plan

The QuoVadis Business Continuity Plan is strictly confidential and provides for:

- Incident and compromise handling procedures;
- Computing resources, software, and/or corrupted data handling procedures;
- Entity private key compromise procedures; and
- Entity public key revocation procedures; and
- Business continuity capabilities and procedures after a disaster.

5.8. CA And/Or RA Termination

In case of termination of CA operations, QuoVadis will provide timely notice and transfer of responsibilities to

6.2.10. Method Of Destroying Private Key

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

All Digital Certificate Holders have an obligation to protect their private keys from compromise. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure or unauthorised use.

Upon expiration of a key pair's allowed lifetime, or upon CA termination, QuoVadis personnel shall destroy the CA private key by deleting and overwriting the data (e.g., via re-initialization or zeroization) or physical destruction (e.g., with a metal shredder or hammer). Such destruction shall be documented.

6.2.11. Cryptographic Module Rating

The cryptographic modules used by the QuoVadis PKI are validated to FIPS 140-2 Level-3 security standards.

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. The validity period of Certificates will be dependent on the Certificate Policy in question.

6.3.2. Certificate Operational Periods And Key Pair Usage Periods

The maximum validity periods for Certificates issued within the QuoVadis PKI are:

Root CA Certificate	25 years
Issuing CA Certificates	10 years
Business SSL Certificates	3 years
EV SSL Certificates	2 years

6.4. Activation Data

6.4.1. Activation Data Generation And Installation

Two-factor authentication shall be used to protect access to a private key. One of these factors must be randomly and automatically generated.

6.4.2. Activation Data Protection

No activation data other than access control mechanisms is required to operate cryptographic modules. Personal Identification Codes 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. Activation data should be memorized, not written down. Activation data must never be shared. Activation data must not contain the user's personal information.

6.4.3. Other Aspects Of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

QuoVadis has a formal Information Security Policy that documents the QuoVadis policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

Computer security technical requirements are achieved utilising a combination of hardened security modules and software, operating system security features, PKI and CA software and physical safeguards, including security Policies

6.5.2. Computer Security Rating

The QuoVadis approved Information Security Policy incorporates computer security ratings that are specific to QuoVadis. QuoVadis computer security ratings are achieved and maintained by real time security monitoring and analysis, monthly security reviews by the QuoVadis Chief Security Officer, and annual security reviews by external auditors.

6.6. Life Cycle Technical Controls

All hardware and software procured for the QuoVadis PKI must be purchased in a manner that will mitigate the risk that any particular component was tampered with, such as random selection of specific components. Equipment developed for use within the QuoVadis PKI shall be developed in a controlled environment under strict change control procedures.

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

6.6.1. System Development Controls

QuoVadis follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke, and manage public key Certificates, such as X.509 public key Certificates. The CIMC is based on the Common Criteria/ISO IS15408 standards.

6.6.2. Security Management Controls

QuoVadis follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke, and manage public key Certificates, such as X.509 public key Certificates. The CIMC is based on the Common Criteria/ISO IS15408 standards.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

7.1.1. Version Numbers

Information for interpreting Certificate and CRL Profiles may be found in IETF RFC 2459. QuoVadis Certificates

7.3. Online Certificate Status Protocol Profile

OCSP is enabled for all Certificates within the QuoVadis PKI.

7.3.1. Online Certificate Status Protocol Version Numbers

OCSP Version 1, as defined by RFC 2560, is supported within the QuoVadis PKI.

7.3.2. Online Certificate Status Protocol Extensions

No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency, Circumstance And Standards Of Assessment

The practices specified in this CP/CPS have been designed to meet or exceed the requirements of, and QuoVadis is audited for compliance to, generally accepted and developing industry standards including:

- AICPA/CICA WebTrust for Certification Authorities and the WebTrust Extended Validation Program;
- Bermuda Authorised Certification Service Provider standards of the Bermuda electronic Transactions Act;
- Swiss Zert ES Qualified Certification Service Providers standards (ZertES), including adherence to ETSI 101.456 TS and other specifications

8.2. Identity And Qualifications Of Assessor

The audit services described in Section 8.1 are performed by independent, recognised, credible, and established audit firms having significant experience with PKI and cryptographic technologies. The WebTrust and Bermuda Certificate Service Provider audits have been carried out by Ernst & Young. The accreditation audits for Swiss and ETSI requirements have been performed by KPMG AG.

8.3. Assessor's Relationship To Assessed Entity

9.1.3. Revocation Or Status Information Access Fees

QuoVadis does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of a QuoVadis issued Certificate through the use of CRLs. QuoVadis reserves the right to establish and charge a reasonable fee for providing Certificate status information services via OCSP.

9.1.4. Fees For Other Services

No stipulation.

9.1.5. Refund Policy

QuoVadis may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. Financial Responsibilities

9.2.1. Financial Records

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

9.2.2. No Partnership or Agency

Certificate Holder shall not represent itself as being the affiliate nor an agent, partner, employee or representative of QuoVadis and shall not hold itself out as such nor as having any power or authority to incur any obligation of any nature express or implied on behalf of QuoVadis and nothing in this Agreement shall operate nor be construed so as to constitute Certificate Holder as an agent, partner, employee, or representative of QuoVadis.

9.2.3. Insurance Cover

QuoVadis maintains the following insurance related to its respective performance and obligations:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

9.2.4. Other Assets

No stipulation.

9.2.5. Insurance Or Warranty Coverage For End-Entities

Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the private key that corresponds to the public key in their QuoVadis Certificate. Relying Parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.3. Confidentiality Of Business Information

9.3.1. Scope Of Confidential Information

QuoVadis keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys;
- Any activation data used to access private keys or gain access to the CA system;
- Any business continuity, incident response, contingency, and disaster recovery plans;
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information;
- Any information held by QuoVadis as private information in accordance with Section 9.4;
- Any transactional, audit log, and archive records including Certificate Application records and documentation submitted in support of Certificate Applications whether successful or rejected; and
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS)

- Providing the operational infrastructure and certification services, including the Repository;
- Making reasonable efforts to ensure it conducts and efficient and trustworthy operation;
- Maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation; and
- Investigating any suspected compromise which may threaten the integrity of the QuoVadis PKI.

QuoVadis hereby warrants (i) it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue (ii) Certificates shall be revoked if QuoVadis believes or is notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

QuoVadis makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

Upon accepting a Certificate the Certificate Holder represents to QuoVadis and to Relying Parties that at the time of

- Any liability that arises from security, usability, in tegrity of products, including hardware and software a

- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of QuoVadis and/or its subcontractors or service providers; or
- One or more of the following events: a natural disaster or Act of God (including without limitation flood,

means of providing any notice required pursuant to this CP/CPS to QuoVadis unless specifically provided otherwise (for example in respect of revocation procedures).

9.12. Amendments

9.12.1. Procedure For Amendment

Amendments to this CP/CPS are made and approved by the QuoVadis Policy Management Authority (PMA). Amendments shall be in the form of an amended CP/CPS or a replacement CP/CPS. Updated versions of this CP/CPS supersede any designated or conflicting provisions of the referenced version of the CP/CPS.

9.12.2. Notification Mechanism And Period

The QuoVadis PMA reserves the right to amend this CP/CPS without notification for amendments that are not material, including typographical corrections, changes to URLs, and changes to contact details. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the QuoVadis PMA.

9.12.3. Circumstances Under Which OID Must Be Changed

Unless the QuoVadis PMA determines otherwise, the OID for this CP/CPS shall not change. If a change in QuoVadis' certification practices is determined by the PMA to warrant a change in the currently specified OID for a particular Certificate Policy, then the revised version of this CP/CPS will also contain a revised OID for that Certificate Policy.

9.13. Dispute Resolution Provisions

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a "participant" within the QuoVadis PKI) arising out of or relating to this QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

9.14. Governing Law

This CP/CPS and any QuoVadis Certificates issued by QuoVadis are governed by the laws of the country referred to in the Certificate Holder Agreement for the Certificate in question, without reference to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods. Venue with respect to any dispute, controversy, or claim shall under the laws of the country referred to in the Certificate Holder Agreement for the Certificate in question.

9.15. Compliance With Applicable Law

Certificate Holders and Relying Parties shall use QuoVadis Certificates and any other related information and materials provided by QuoVadis only in compliance with all applicable laws and regulations. QuoVadis may refuse to issue or may revoke Certificates if, in the reasonable opinion of QuoVadis, issuance or the continued use of the QuoVadis Certificates would violate applicable laws or regulations.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Not Applicable.

9.16.3. Assignment

Parties to this CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of QuoVadis, and any such attempted assignment shall be void.

9.16.4. Severability

9.16.6. Force Majeure

QUOVADIS ACCEPTS NO LIABILITY FOR ANY BREACH OF WARRANTY, DELAY, OR FAILURE IN PERFORMANCE THAT RESULTS FROM EVENTS BEYOND ITS CONTROL SUCH AS ACTS OF GOD, ACTS OF WAR, ACTS OF TERRORISM, EPIDEMICS, POWER OR TELECOMMUNICATION SERVICES FAILURE, FIRE, AND OTHER NATURAL DISASTERS.

9.17. Other Provisions

No stipulation.

QuoVadis Global SSL ICA

Field	Value
Version	V3
Serial Number	Unique number 057a
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 1/12/2007 12:13 PM NotAfter: 1/12/2017 12:13 PM
Subject Distinguished Name	

Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 2 Certification Policies and Certificate Practice Statement.
Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL = http://ocsp.quovadisglobal.com
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/QVSSLICA.crl

Purposes of Business SSL
QuoVadis Business SSL Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. The primary purposes of a Business SSL Certificate are to:

- Identify the individual or entity that controls a website; and
- Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the Certificate is actively engaged in doing business;
- That the Subject named in the Certificate complies with applicable laws;
- That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the Certificate.

Eligible Applicants
Individuals (natural persons), incorporated entities, government entities, general partnerships, unincorporated associations, and sole proprietorships may apply for QuoVadis Business SSL Certificates.

Verification Requirements
Before issuing a Business SSL Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and has accepted a Certificate Holder Agreement for the requested Certificate.

Documentation requirements for organisation Applicants may include:

- Certificate of Incorporation (or analogous document); or
- Memorandum of Association (or analogous document); or
- Articles of Incorporation (or analogous document); or
- Business License (or analogous document); or
- Any power of attorney or other authority pursuant to which this Application has been signed.

Government and not-for-profit entities may provide information on letterhead from the Head of the Department confirming the organisation's contact details and proof of right.

Documentation requirements for individual Applicants may include trustworthy, valid photo ID issued by a Government Agency (such as a passport).

QuoVadis may accept at its discretion other official documentation supporting an application. QuoVadis may also use

Extended Validation SSL

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique number	
Issuer Signature Algorithm	sha-1WithRSAEncryption(1.2.840.113549.1.1.5)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Global SSL ICA OU = www.quovadisglobal.com O = QuoVadis Limited C = BM	
Validity Period	1 or 2 years expressed in UTC format	
Subject Distinguished Name		
Organization Name	subject:organisationName (2.5.4.10)	This field MUST contain the Subject's full legal organisation name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organisation name in parenthesis. If the combination of the full legal organisation name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organisation name will be used.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard Certificates are not allowed for EV Certificates.
City or Town of Incorporation	subject:jurisdictionOfIn corporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows.

State/Province of Incorporation	subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	ASN.1 - X520StateOrProvinceName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above.
Country of Incorporation	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)	ASN.1 - X520countryName as specified in RFC 5280 Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code.
Registration Number	Subject:serialNumber (2.5.4.5)	For Private Organisations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number or verifiable date of creation, the field will contain the label “Government Entity”.
Business Category	Subject:businessCategory (2.5.4.15)	This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject.
Number & street (optional)	subject:streetAddress (2.5.4.9)	
City or town	subject:localityName (2.5.4.7)	
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	
Country	subject:countryName (2.5.4.6)	
Postal code (optional)	subject:postalCode (2.5.4.17)	
Subject Public Key Information	1024 or 2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Issuer’s Signature	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)	
Extension	Value	
Authority Key Identifier	c=no; Octet String – Same as Issuer's 32 4d a1 4f ea f0 ae 99 b6 ee 9b 07 2c 84 08 11 50 8b e2 7e	

Trusted Code Signing

Step 5: QuoVadis obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the Certificate Request and notify the Applicant accordingly. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 6: QuoVadis creates the Trusted Code Signing Certificate.

Step 7: The Certificate is delivered to the Applicant.

Renewal
Renewal requirements and procedures include verification that the Applicant continues to have authority to publish