QUOVADIS ROOT CA2
CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT

OID: 1.3.6.1.4.1.8024.0.2
Effective Date: 12 January 2007
Version: 1.7

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

1. INTRODUCTION

1.1. Overview

QuoVadis SSL Certificates (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.

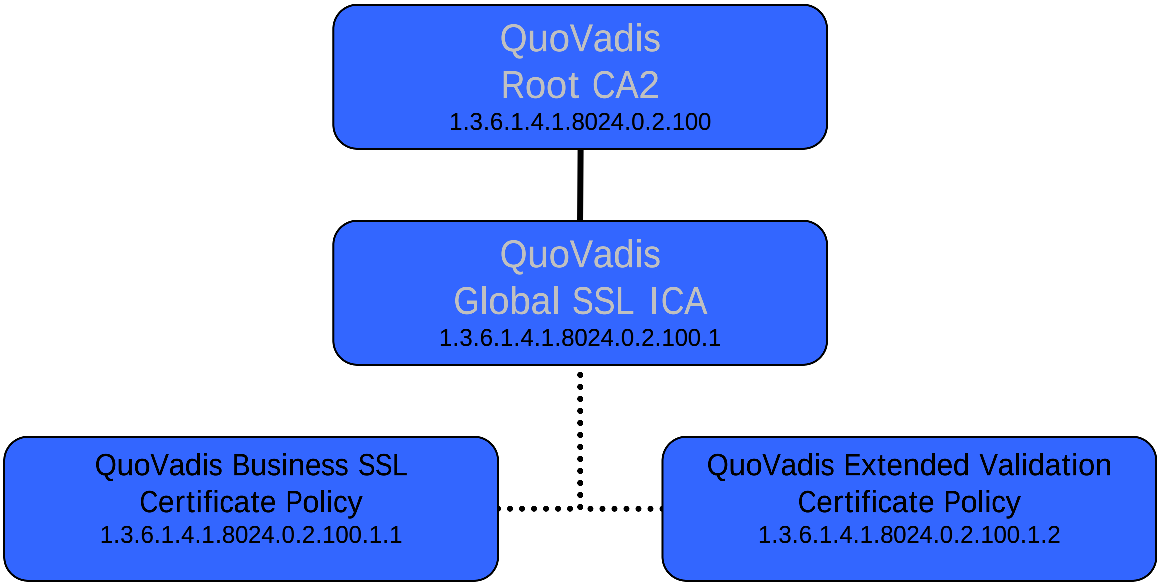
This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that QuoVadis Root CA2 uses in the generation, issue, use, and management of Certificates and serves to notify Subscribers and Relying Parties of their roles and responsibilities concerning Certificates.

QuoVadis ensures the integrity of its Public Key Infrastructure (PKI) operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between QuoVadis and any Participant in the QuoVadis PKI. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation.

QuoVadis issues two forms of Certificate according to the terms of this CP/CPS:

i. Business SSL are Certificates for which limited authentication and authorization checks are performed on the Subscriber and the individuals acting for the Subscriber.

ii. Extended Validation SSL are Certificates issued in compliance the “Guidelines for Extended Validation Certificates” (EV Guidelines) published by the CA/Browser Forum. The EV Guidelines are intended to provide enhanced assurance of identity of the Subscriber by enforcing uniform and detail



QuoVadis Root CA2 and the QuoVadis Global SSL ICA issue Certificates to Subscribers in accordance with this CP/CPS. In its role as a CA, QuoVadis performs functions associated with public key operations that include receiving requests; issuing, revoking and renewing a Certificate; and the maintenance, issuance, and publication of CRLs for users within the QuoVadis PKI. In its capacity as a CA, QuoVadis will:

- Conform its operations to this CP/CPS (or other relevant business practices);
- Issue and publish Certificates in a timely manner;
- Perform verification of Subscriber information in accordance with this CP/CPS;
- Revoke Certificates upon receipt of a valid request from an authorized person; and
- Notify Subscribers of the imminent expiry of their Certificates.

1.3.2. Registration Authorities
Not applicable.

1.3.3. Certificate Subscribers
Subscribers are individuals, companies, or organizations that use PKI in relation with QuoVadis supported transactions and communications. Subscribers are parties that are identified in a Certificate and hold the private key corresponding to the public key that is listed in the Certificate. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant for QuoVadis services.

Before accepting and using a Certificate, a Subscriber must: (i) generate its own key pair; (ii) submit an application for a QuoVadis Certificate; and (iii) accept and agree to the terms and conditions of the applicable QuoVadis Subscriber Agreement. Subscriber is solely responsible for the generation of the key pair to which its QuoVadis Certificate relates and for the protection of the Private Key underlying the QuoVadis Certificate. Subscriber shall post the Security Statement provided by QuoVadis on Subscriber's website and shall immediately notify QuoVadis if any information contained in a QuoVadis Certificate changes or becomes false or misleading, or in the event that its private key has been compromised or Subscriber suspects that it has been compromised. A Subscriber must immediately stop using a Certificate and delete from the Subscriber's server upon revocation or expiration.

ity

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate.

1.4.2. Prohibited Certificate Usage

QuoVadis Certificates may not be used and no participation is permitted in the QuoVadis PKI (i) in circumstances that breach, contravene, or infringe the rights of others; or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental

Contract Signer: A Contract Signer is a natural person who is employed by the Applicant and who has express authority to sign Subscriber Agreements on behalf of the Applicant.

Participants: A Participant is an individual or entity within the QuoVadis PKI and may include CAs and their Subsidiaries and Holding Companies; Subscribers including Applicants; and Relying Parties.

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 of issued and revoked Certificates.

Subscriber: The entity that has been issued a Certificate; the Subject of a Certificate.

Subscriber Agreement: The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the class of Certificate.

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
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY 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 Subscribers 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

3.2.2. Authentication Of Organisation Identity

Authentication of Organisation identity is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B.

3.2.3. Authentication Of Individual Identity

Where applicable, authentication of Individual identity is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B.

3.2.4. Non-Verified Certificate Holder Information

QuoVadis does not include unconfirmed Subscriber information in Certificates.

3.2.5. Validation Of Authority

Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B.

For Certificates issued at the request of a Subscriber's Agent, both the Agent and the Subscriber shall jointly and severally indemnify and hold harmless QuoVadis, and its parent companies, subsidiaries, directors, officers, and employees. The Subscriber shall control and be responsible for the data that an Agent of Subscriber supplies to QuoVadis. The Subscriber must promptly notify QuoVadis of any misrepresentations and omissions made by an Agent of Subscriber.

3.3. Identification And Authentication For Re-Key Requests

3.3.1. Identification And Authentication For Routine Re-Key

Identification and Authentication procedures are the same for re-key as for a new application. Key pairs must always expire at the same time as the associated Certificate.

3.3.2. Identification and Authentication For Re-Key After Revocation

After revocation, a Subscriber must submit a new application.

3.4. Identification and Authentication For Revocation Requests

See Section 4.9 for information about Certificate Revocation procedures.

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. Certificate Application

The process to apply for QuoVadis Certificates varies by class of Certificate and is described in Appendix B.

4.2. Certificate Application Processing

4.2.1. Performing Identification And Authentication Functions

During application processing, QuoVadis Validation Specialists employ controls to validate the identity of the Subscriber and other information featured in the certificate application to ensure compliance with this CP/CPS.

4.2.2. Approval Or Rejection Of Certificate Applications

From time to time, QuoVadis may modify the requirements related to application information requested, based on QuoVadis requirements, business context of the usage of Certificates, or as may be required by law or changes to the EV Guidelines.

QuoVadis, in its sole discretion, may refuse to accept an application for a Certificate or for the renewal of a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. QuoVadis reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3. Time To Process Certificate Applications

QuoVadis makes reasonable efforts to confirm certificate application information and issue a Certificate within a reasonable time frame, which is dependent on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, QuoVadis aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within three working days.

From time to time, events outside of the control of QuoVadis may delay the issuance process. However, QuoVadis will make every reasonable effort to meet its issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

- A QuoVadis CA Private Key used to issue that Certificate has been compromised;
- QuoVadis' right to issue and manage EV Certificates under the EV Guidelines expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository); or
- QuoVadis ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

4.9.2. Who Can Request Revocation

QuoVadis may revoke any Certificate issued within the QuoVadis PKI at its sole discretion. The Subscriber and its

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 support suspension of Certificates.

4.9.14. Who Can Request Suspension

The QuoVadis PKI does not support suspension of Certificates.

5.1.4. Water Exposures

The QuoVadis secure operating area provides protection against water.

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 11 (eleven) years for audit trail files and for key and Certificate information. Audit logs are stored until at least 11 (eleven) years after the QuoVadis Issuing CA ceases operation.

5.4.4. Protel7i7( )]TJ-0.0003 Tc 0.0011 Tw -25.76 n(Se /2e(Protel)1 TwT[lP <MCID 34 >6 n(Se / wi[opdatedClSe /

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 authorized 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) Subscriber 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 11 (eleven) 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 resumption plan as proprietary and that it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.

6.1.5. Key Sizes

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.

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 class of Certificate 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

Wildcard certificates may not be issued under the EV Guidelines.

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

6.6. Life Cycle Technical Controls

7.1.2. Certificate Extensions

See Appendix A and Appendix B.

7.1.3. Algorithm Object Identifiers

See Appendix A and Appendix B.

7.1.4. Name Forms

See Appendix A and Appendix B.

7.1.5. Name Constraint B.

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 Provider standards (ZertES), including adherence to ETSI 101.456TS 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 Klynveld Peat Marwick Goerdeler SA.

8.3. Assessor's Relationship To Assessed Entity

QuoVadis and the auditors do not have any other relationship that would impair their 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.

8.4. Topics Covered By Assessment

Topics covered by the annual audits of QuoVadis include but are not limited to CA business practices disclosure (i.e., this CP/CPS), the service integrity of QuoVadis' CA operations, the environmental controls that QuoVadis implements to ensure trustworthy systems, and QuoVadis' compliance with relevant laws, regulations, and guidelines.

8.5. Actions Taken As A Result Of Deficiency

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by QuoVadis with input from auditors. QuoVadis at its sole discretion will determine an appropriate course of action and time frame to rectify the deficiency.

8.6. Publication Of Audit Results

The results of these audits in the form of publicly available audit reports or opinions as provided by the external auditors responsible for these audits are published on the QuoVadis website or are available upon request.

8.7 Self Audits

QuoVadis also controls its service quality by performing ongoing self audits against a randomly selected sample of Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance Or Renewal Fees

QuoVadis charges Subscriber fees for verification, issuance, and renewal. Such fees are detailed on the QuoVadis web site. QuoVadis retains its right to effect changes to such fees. QuoVadis customers will be suitably advised of price amendments as detailed in relevant customer agreements.

9.1.2. Certificate Access Fees

QuoVadis reserves the right to establish and charge a reasonable fee for access to its Repository.

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

9.4.1. Privacy Plan

QuoVadis has implemented a privacy policy in compliance with this CP/CPS. The QuoVadis privacy policy is published on the QuoVadis web site.

9.4.2. Information Treated As Private

Personal information about an individual that is not publicly available in the contents of a Certificate or CRL is considered private.

9.4.3. Information Deemed Not Private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private. This QuoVadis CP/CPS is a public document and is not confidential information and is not treated as private.

9.4.4. Responsibility To Protect Private Information

Information supplied to QuoVadis as a result of the practices described in this CP/CPS may be covered by national government or other privacy legislation or guidelines. QuoVadis will not divulge any private personal information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

9.4.5. Notice And Consent To Use Private Information

In the course of accepting a Certificate, individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the QuoVadis CA, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure Pursuant To Judicial Or Administrative Process

As a general principle, no document or record belonging to QuoVadis is released to law enforcement agencies, officials, or persons relating to civil discovery proceedings 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 a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable.

9.5. Intellectual Property Rights

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.

Certificates are the exclusive property of QuoVadis. QuoVadis gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. QuoVadis reserves the right to revoke a Certificate at any time and at its sole discretion. Private keys and public keys are the property of the applicable Subscribers who rightfully issue and hold them.

This QuoVadis CP/CPS and the Proprietary Marks are the intellectual property of QuoVadis. QuoVadis retains exclusive title to, copyright in, and the right to license this QuoVadis CP/CPS. QuoVadis excludes all liability for breach of any other intellectual property rights.

9.6. Representations And Warranties

QuoVadis discharges its obligations by:

- 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.

9.6.1. RA Representations and Warranties

Not applicable.

9.6.2. Subscriber Representations And Warranties

As part of the Subscriber Agreement agreed to by all Subscribers, the following commitments and warranties are made for the express benefit of QuoVadis and all Relying Parties and Application Software Vendors:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to QuoVadis, both in the EV Certificate Request and as otherwise requested by QuoVadis in connection with the issuance of the Certificate(s) to be supplied by QuoVadis;
- Protection of Private Key: An obligation and warranty by the Subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated access information or device such as a password or token);
- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- Use of Certificate: An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an Certificate and its associated Private Key, and promptly request that QuoVadis revoke the Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the Certificate; and
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an Certificate upon expiration or revocation of that Certificate.

Without limiting other Subscriber obligations stated in this CP/CPS, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a certificate the Subscriber represents to QuoVadis and to Relying Parties that at the time of acceptance and until further notice:

- The Subscriber retains control of the Subscriber's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person

- Rely on a QuoVadis Certificate only as may be reasonable under the circumstances, given (i) the Relying Party's not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the QuoVadis ch damages, rD9r.u5 dvi

9.10.2. Termination

This CP/CPS shall remain in force until it is amended or replaced by a new version in accordance with this Section 9.10.

9.10.3. Effect Of Termination And Survival

The conditions and effect resulting from termination of this CP/CPS will be communicated via the QuoVadis website upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11. Individual Notices And Communications With Participants

Electronic mail, postal mail, fax, and web pages will all be valid means of QuoVadis providing any of the notices required by this CP/CPS, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid 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 reserve 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 determine 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 class of Certificate, then the revised version of this CP/CPS will also contain a revised OID for that class of Certificate.

9.13. Dispute Resolution Provisions

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall

APPENDIX A – Root and Issuing CA Profiles

QuoVadis Root CA2

Field	**Value**
Version	V3
Serial Number	Unique number 0509
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	25 years expressed in UTC format NotBefore: 11/24/2006 2:27 PM NotAfter: 11/24/2031 2:23 PM

Subject Distinguished Name	CN = QuoVadis Root CA 2
	O =QuoVadis Limited
	C = BM

Subject Public Key Information	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 4096 bits
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**

Authority Key Identifier	c=no;
	KeyID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
	Certificate Issuer:
	Directory Address:
	CN=QuoVadis Root CA 2
	O=QuoVadis Limited
	C=BM
	Certificate SerialNumber=05 09

Subject Key Identifier	c=no; 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Key Usage	c=no; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=None
Key Id Hash(sha1):	73 97 82 ea b4 04 16 6e 25 d4 82 3c 37 db f8 a8 12 fb cf 26
Cert Hash(md5):	5e 39 7b dd f8 ba ec 82 e9 ac 62 ba 0c 54 00 2b

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	CN = QuoVadis Global SSL ICA
	OU = www.quovadisglobal.com
	O = QuoVadis Limited
	C = BM

Subject Public Key Information	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;
	KeyID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b

Subject Key Identifier	c=no; 32 4d a1 4f ea f0 ae 99 b6 ee 9b 07 2c 84 08 11 50 8b e2 7e
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	c=no; Certificate Policies; {All issuance policies } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/cps
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=None
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/QVRCA2.crl
Key Id Hash(sha1):	bf f0 f0 22 bf 96 30 fc 96 69 a0 07 76 19 01 f3 de 98 4c 4b
Cert Hash(md5):	df 31 69 f3 8a 73 b1 14 74 f2 76 1a 8a 0d 50 d8
Cert Hash(sha1):	c4 e2 6d b5 fb 5e 8b 57 05 aa 7a 5d b9 39 44 e3 66 8e 12 7d Tw V9.9t5 n0004 8 0 .489g Tw V9.9t5 n0004 8 a

Appendix B – Subscriber Certificate Profiles

Business SSL

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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://trust.quovadisglobal.com/QVSSLICA.crt
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-base 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 behavior of the Subject. As suchtity of the Subject named in tV

Step 2: QuoVadis independently verifies all information using a variety of sources.

Step 4: The Contract Signer accepts the Subscriber Agreement and approves certificate issuance.

Step 5: All signatures by Certificate Requesters and Contract Signers are verified through follow-up procedures or telephone calls.

Step 6: 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 reaso

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:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating 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 organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 3280, only the full legal organization name will be used.

State/Province of Incorporation	subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	ASN.1 - X520StateOrProvinceName as specified in RFC 3280 Full name of Jurisdiction of Incorporation for an Incorporating 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 3280 Jurisdiction of Incorporation for an Incorporating 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)	This field MUST contain the unique Registration Number assigned to the Subject by the Incorporating Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only)
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	
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	
Key Usage	c=yes;	

Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.2 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/cps [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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://trust.quovadisglobal.com/QVSSLICA.crt	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/QVSSLICA.crl	

Purpose of EV SSL

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

- Identify the legal entity that controls a website;
- Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number; 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.

EV SSL also help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence; provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud; and assist law enforcement in investigations including where appropriate, contacting, investigating, or taking legal action against the Subject.

QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, QuoVadis 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.

Commitment to Comply with Guidelines

QuoVadis conforms to the current version of the CA/Browser Forum “Guidelines for Extended Validation Certificates” (EV Guidelines) published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

Eligible Subscribers

QuoVadis issues EV Certificates to Private Organization

(a) Private Organization Subjects

- The Private Organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation (e.g., by issuance of a certificate of incorporation);
- The Private Organization MUST have designated with the Incorporating Agency a Registered Agent or Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;
- The Private Organization MUST NOT be designated on the records of the Incorporating Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
- The Private Organization’s Jurisdiction of Incorporation and/or its Place of Business MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a certificate by the laws of the United States; and
- The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the United States.

(b) Government Entity Subjects

- The legal existence of the Government Entity MUST be established by the law of the Jurisdiction of Incorporation;
- The Government Entity MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a certificate by the laws of the United States; and
- The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the United States.

Until additional criteria for validation are defined by the EV Guidelines, QuoVadis cannot issue EV Certificates to any person or any organization or entity that does not satisfy the requirements above, including but not limited to the following:

- General partnerships
- Unincorporated associations
- Sole proprietorships
- Individuals (natural persons)

Additional Warranties and Representations for EV Certificates

QuoVadis makes the following EV Certificate Warranties solely to Certificate Subscribers, Certificate Subjects, Application Software Vendors with whom QuoVadis has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors, and all Relying Parties that actually rely on such EV Certificate during the period when it is valid, that it followed the requirements of the EV Guidelines and this CP/CPS in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (EV Certificate Warranties).

The EV Certificate Warranties specifically include, but are not limited to, warranties that:

- Legal Existence: QuoVadis has confirmed with the Incorporating Agency in the Subject’s Jurisdiction of Incorporation that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;

- Identity: QuoVadis has confirmed that, as of the date the EV Certificateshwas-issued, the legal name of the ing: 0.06d[(e wa

- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with QuoVadis that satisfies the requirements of the EV Guidelines;

- Status: QuoVadis will follow the requirements of the EV Guidelines and maintains a 24/7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or Revoked; and

- Revocation: QuoVadis will follow the requirements of the EV Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in the EV Guidelines.

Verification Requirements

Before issuing an EV Certificate, QuoVadis ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended accomplish the following:

i. Verify Applicant's existence and identity, including;
    - Verify Applicant's legal existence and identity (as established with an Incorporating Agency),
    - Verify Applicant's physical existence (busin

Subscriber Obligations

Each Applicant must enter into a Subscriber Agreement with QuoVadis which specifically names both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf, and contains provisions imposing on the Applicant the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the QuoVadis, both in the EV Certificate Request and as otherwise requested by the QuoVadis in connection with the issuance of the EV Certificate(s) to be supplied by the QuoVadis;

- Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device – e.g., password or token);

- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;

- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request the QuoVadis to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate; and

- Termination of Use of EV Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

Application Process

During the certificate approval process, QuoVadis Validation Specialists employ controls to validate the identity of the Subscriber and other information featured in the certificate application to ensure compliance with the Guidelines.

Step 1: The Certificate Requester provides a signed certificate application to QuoVadis, which includes information about the Applicant as well as personnel within the organization who have authority to approve the request and sign the Subscriber Agreement. In addition, the Certificate Requester provides a PKCS#10 CSR as well as billing information for processing the request and issuing the EV Certificate.

Step 2: QuoVadis independently verifies all information that is required to be verified by the EV Guidelines using a variety of sources.

Step 3: QuoVadis requests and receives a signed EV Authority Letter from the Applicant (unless a valid EV Authorization Letter from the Applicant is already in its possession).

Step 4: The Contract Signer signs the Subscriber Agreement.

Step 5: The Certificate Approver is contacted to obtain approval of certificate issuance.

Step 6: All signatures by Certificate Requesters, Certificate Approvers and Contract Signers are verified through follow-up procedures or telephone calls.

Step 7: QuoVadis obtains and documents further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, and/or other sources of information as necessary to resolve discrepancies or details requiring further explanation. QuoVadis procedures ensure that a second Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the EV Certificate and looks for discrepancies or other details requiring further explanation. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 8: QuoVadis creates the EV Certificate.