



**QUOVADIS ROOT CA2  
CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT**

**OID: 1.3.6.1.4.1.8024.0.2  
Effective Date: 02 October 2007  
Version: 1.8**

Copyright © QuoVadis 2007. All rights reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by QuoVadis.

## 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.quovadis.bm](http://www.quovadis.bm)  
Electronic mail: [policy@quovadis.bm](mailto:policy@quovadis.bm)

### Version Control:

<i>Author</i>	<i>Date</i>	<i>Version</i>	<i>Comment</i>
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

## Table of Contents

<b>1. INTRODUCTION</b>	<b>1</b>
1.1. Overview	1
1.2. Document Name And Identification	1
1.3. PKI Participants	1
1.5. Policy Administration	3
1.6. Definitions and Acronyms	3
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES</b>	<b>4</b>
2.1. Repositories	4
2.2. Publication of Certificate Information	4
2.3. Time or Frequency of Publication	5
2.4. Access Controls on Repositories	5
<b>3. IDENTIFICATION AND AUTHENTICATION</b>	<b>5</b>
3.1. Naming	5
3.2. Initial Identity Validation	6
3.3. Identification And Authentication For Re-Key Requests	6
3.4. Identification and Authentication For Revocation Requests	6
<b>4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS</b>	<b>6</b>
4.1. Certificate Application	6
4.2. Certificate Application Processing	6
4.3. Certificate Issuance	7
4.4. Certificate Acceptance	7
4.5. Key Pair And Certificate Usage	8
4.6. Certificate Renewal	8
4.7. Certificate Re-Key	8
4.8. Certificate Modification	8
4.9. Certificate Revocation And Suspension	8
4.10. Certificate Status Services	10
4.11. End Of Subscription	10
4.12. Key Escrow And Recovery	10
<b>5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS</b>	<b>10</b>
5.1. Physical Controls	11
5.2. Procedural Controls	11
5.3. Personnel Controls	12
5.4. Audit Logging Procedures	13
5.5. Records Archival	14
5.6. Key Changeover	15
5.7. Compromise And Disaster Recovery	15
5.8. CA And/Or RA Termination	15
<b>6. TECHNICAL SECURITY CONTROLS</b>	<b>16</b>
6.1. Key Pair Generation And Installation	16
6.2. Private Key Protection And Cryptographic Module Engineering Controls	16
6.3. Other Aspects Of Key Pair Management	17
6.4. Activation Data	17
6.5. Computer Security Controls	18
6.6. Life Cycle Technical Controls	18
6.7. Time-Stamping	19
<b>7. CERTIFICATE, CRL, AND OCSP PROFILES</b>	<b>19</b>
7.1. Certificate Profile	19
7.2. CRL Profile	20
7.3. Online Certificate Status Protocol Profile	20
<b>8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS</b>	<b>20</b>
8.1. Frequency, Circumstance And Standards Of Assessment	20
8.2. Identity And Qualifications Of Assessor	20
8.3. Assessor's Relationship To Assessed Entity	20
8.4. Topics Covered By Assessment	20

8.5.	Actions Taken As A Result Of Deficiency .....	21
8.6.	Publication Of Audit Results.....	21
8.7	Self Audits.....	21
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS.....</b>	<b>21</b>
9.1.	Fees .....	21
9.2.	Financial Responsibilities .....	21
9.3.	Confidentiality Of Business Information.....	22
9.4.	Responsibility To Protect Private Information .....	22
9.5.	Intellectual Property Rights .....	23
9.6.	Representations And Warranties.....	23
9.7.	Disclaimers Of Warranties .....	24
9.8.	QuoVadis Liability .....	25
9.9.	Indemnities.....	26
9.10.	Term And Termination .....	26
9.11.	Individual Notices And Communications With Participants .....	27
9.12.	Amendments.....	27
9.13.	Dispute Resolution Provisions.....	27
9.14.	Governing Law .....	27
9.15.	Compliance With Applicable Law.....	27
9.16.	Miscellaneous Provisions .....	27
9.17.	Other Provisions .....	28
<b>APPENDIX A – Root and Issuing CA Profiles .....</b>	<b>29</b>	
QuoVadis Root CA2.....	29	
QuoVadis Global SSL ICA.....	30	
<b>Appendix B – Subscriber Certificate Profiles .....</b>	<b>31</b>	
Business SSL .....	31	
Extended Validation SSL.....	34	

## 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 the Issuance and Management of 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 detailed validation procedures across all EV-issuing CAs.

QuoVadis Certificates comply with Internet standards (x509 v.3) as set out in RFC 3280. This CP/CPS follows the IETF PKIX RFC 3647 framework with 9 sections that cover practices and procedures for identifying Certificate applicants; issuing and revoking Certificates; and the security controls related to managing the physical, personnel, technical, and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some sections will have the statement "Not applicable" or "No Stipulation."

### 1.2. Document Name And Identification

This document is the QuoVadis Root CA2 CP/CPS which was adopted by the QuoVadis Policy Management Authority (PMA). The Document Object Identifier (OID) assigned to this CP/CPS is 1.3.6.1.4.1.8024.0.2.

The provisions of this CP/CPS, as amended from time to time, are incorporated by reference into all QuoVadis Certificates that are issued on or after the effective date of publication of this CP/CPS. QuoVadis shall make amendments to this CP/CPS in accordance with Section 9.10.

### 1.3. PKI Participants

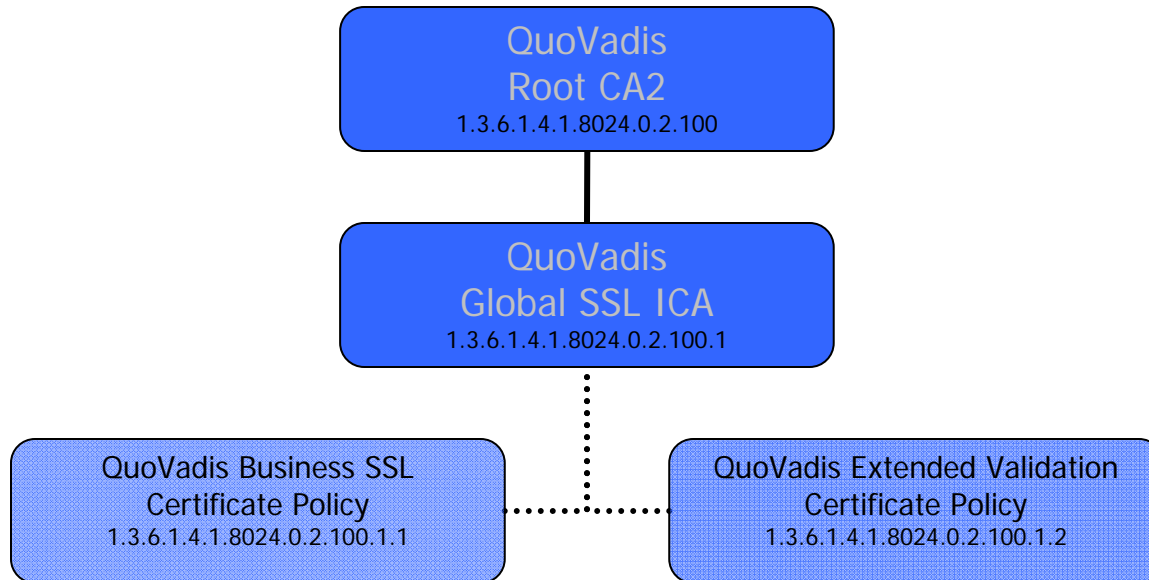
Participants (Participants) within the QuoVadis PKI include:

- Certification Authorities (Root and Issuing);
- Registration Authorities ("RA") and Local Registration Authorities ("LRA");
- Certificate Subscribers including Applicants for Certificates prior to Certificate issuance; and
- Relying Parties.

#### 1.3.1. Certification Authority

The following OIDs are pertinent to this CP/CPS:

QuoVadis Root CA2	1.3.6.1.4.1.8024.0.2.100
QuoVadis Global SSL ICA	1.3.6.1.4.1.8024.0.2.100.1
QuoVadis Business SSL	1.3.6.1.4.1.8024.0.2.100.1.1
QuoVadis Extended Validation SSL	1.3.6.1.4.1.8024.0.2.100.1.2



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 authorised person; and
- Notify Subscribers of the imminent expiry of their Certificates.

### **1.3.2. Registration Authorities**

QuoVadis acts as Registration Authority (RA) for Certificates it issues. An RA is an entity that performs verification of Subscriber 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.

### **1.3.3. Certificate Subscribers**

Subscribers are individuals, companies, or organisations 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. A Subscriber shall post the Security Statement provided by QuoVadis on the 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 the Subscriber suspects that it has been compromised. A Subscriber must immediately stop using a Certificate and delete it from the Subscriber's server upon revocation or expiration.

### **1.3.8. Relying Parties**

Relying Parties are Individuals or Organisations who reasonably rely on QuoVadis Certificates in accordance with the terms and conditions of this CP/CPS and all applicable laws and regulations.

Before relying on or using a QuoVadis Certificate, Relying Parties are advised to: (i) read this CP/CPS in its entirety; (ii) visit the QuoVadis Repository to determine whether the Certificate has expired or been revoked and to find out more information concerning the Certificate; and (iii) make their own judgment as to whether and to what degree to rely upon a Certificate.

## **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 order; or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

No reliance may be placed on Certificates and Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use; (ii) in breach of this CP/CPS or the relevant Subscriber Agreement; (iii) in any circumstances where the use of Certificates could lead to death, injury, or damage to property; or (iv) as otherwise may be prohibited by the terms of issue.

## **1.5. Policy Administration**

### **1.5.1. Organisation Administering the CP/CPS**

This CP/CPS and related agreements and security policy documents referenced within this document are administered by the QuoVadis Policy Management Authority (PMA).

*Office Address:*

QuoVadis Limited  
3rd Floor Washington Mall  
7 Reid Street,  
Hamilton HM-11, Bermuda  
Email: [policy@quovadis.bm](mailto:policy@quovadis.bm)

*Mailing Address:*

QuoVadis Limited  
Suite 1640  
48 Par-La-Ville Road  
Hamilton HM-11, Bermuda

### **1.5.2. CP/CPS Approval Procedures**

Approval of this CP/CPS and any amendments hereto is by the QuoVadis PMA. Amendments may be made by updating this entire document or by addendum. The QuoVadis PMA, at its sole discretion, determines whether changes to this CP/CPS require notice or any change in the OID of a Certificate issued pursuant to this CP/CPS.

## **1.6. Definitions and Acronyms**

**Applicant:** The Applicant is an entity applying for a Certificate.

**Authority Letter:** The Authority Letter is a signed by a Confirming Person acting for the Applicant for EV SSL Certificates to establish the authority of individuals to act as the Subscriber's agents.

**Certificate Approver:** A Certificate Approver is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorise other employees or third parties to act as a Certificate Requesters, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

**Certificate Application:** Any of several forms completed by Applicant or QuoVadis and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

**Certificate Requester:** A Certificate Requester is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company), and who completes and submits a Certificate Request on behalf of the Applicant.

**Confirming Person:** A confirming Person is a natural person who must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) who has express authority to sign the QV Authority Letter on behalf of the Applicant.

**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 containing 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
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 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 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 Subscribers require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service, or application that has been confirmed with the Subscriber. QuoVadis may issue Certificates for Intranet use, which may contain entries that are not intended to be relied upon by the general public (e.g., they contain non-standard Top Level Domains, like ".local", or are addressed to an IP number space that has been allocated as private by RFC 1918). Wildcard SSL Certificates have a wildcard asterisk character for the server name in the Subject field. Wildcard EV Certificates may not be issued under the EV Guidelines. The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and, when applicable, the Subject Alternative Name extension.

#### **3.1.2. Need For Names To Be Meaningful**

Distinguished names must be meaningful, unambiguous, and unique. QuoVadis ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field accurately identify the legal entity that is the subject of the Certificate. Similarly, QuoVadis uses non-ambiguous designations in the Issuer field to identify itself as the Issuer of a Certificate (e.g., QuoVadis Global SSL CA).

#### **3.1.3. Pseudonymous Certificate Holders**

QuoVadis does not issue anonymous or pseudonymous Certificates.

#### **3.1.4. Rules For Interpreting Various Name Forms**

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references. In addition, see the Certificate Profiles detailed in Appendix B.

#### **3.1.5. Uniqueness Of Names**

Name uniqueness is ensured through the use of the Common Name attribute of the Subject Field, which contains the authenticated domain name, which is controlled under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN).

#### **3.1.6. Recognition, Authentication, And Role Of Trademarks**

Subscribers shall solely be responsible for the legality of the information they present for use in Certificates issued under this CP/CPS in any jurisdiction in which such content may be used or viewed. Subscribers represent and warrant that when submitting Certificate Requests to QuoVadis and using a domain and distinguished name (and all other Certificate Application information) they do not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other

intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, or to confuse or mislead any person, whether natural or corporate. Subscribers shall defend, indemnify, and hold QuoVadis harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions against QuoVadis.

### **3.2. Initial Identity Validation**

#### **3.2.1. Method To Prove Possession Of Private Key**

The Applicant must submit a digitally signed PKCS#10 Certificate Signing Request (CSR) to establish that it holds the private key corresponding to the public key to be included in a Certificate. QuoVadis parses the PKCS#10 CSR submitted by the Applicant in a secure manner and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR. If any doubt exists, QuoVadis will not perform certification of the key.

#### **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 verify information contained in the Organisation Unit (OU) field in Certificates. Other information may be designated as non-verified in specific Certificate Profiles.

#### **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 the Subscriber supplies to QuoVadis. The Subscriber must promptly notify QuoVadis of any misrepresentations and omissions made by an Agent of the 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 Certificate Policy 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.

### **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 Subscriber 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 Subscriber's computer or cryptographic module according to the Subscriber's system specifications. A Subscriber is deemed to have accepted a Certificate when:

- The Subscriber downloads, installs, or otherwise takes delivery of the Certificate; or
- 30 days pass since issuance of the Certificate.

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT. BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ASSUMES A DUTY TO RETAIN CONTROL OF THE CERTIFICATE'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS, EXCLUSION, MODIFICATION OR UNAUTHORISED USE.

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD QUOVADIS AND ITS AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS, PROCEEDINGS OR CLAIMS, AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS FEES, THAT QUOVADIS, ITS AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE AND THAT ARISE FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE QUOVADIS OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; (III) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY; (IV) USE OF THE CERTIFICATE FOR A PURPOSE WHICH IS LIBELLOUS OR CONSTITUTES MALICIOUS FALSEHOOD OR DISPARAGEMENT OF GOODS OR SERVICES, OR IS OTHERWISE DEFAMATORY, IS IMMORAL, OBSCENE, PORNOGRAPHIC, IS ILLEGAL OR ADVOCATES ILLEGAL ACTIVITY, OR CONSTITUTES A VIOLATION OF PRIVACY OR INFRINGES THE INTELLECTUAL PROPERTY RIGHTS OF QUOVADIS OR A THIRD PARTY.

#### **4.4.2. Publication Of The Certificate By The CA**

All Certificates issued within the QuoVadis PKI are made available in public repositories except where the Subscriber has requested that the Certificate not be published.

#### **4.5. Key Pair And Certificate Usage**

##### **4.5.1. Subscriber Private Key And Certificate Usage**

Subscribers shall protect their private keys from access by unauthorised personnel or other third parties. Subscribers shall use private keys only in accordance with the usages specified in the key usage field extension.

##### **4.5.2. Relying Party Public Key And Certificate Usage**

A Party seeking to rely on a Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement by querying the existence or validity of, or by seeking to place or by placing reliance upon, on a Certificate.

QuoVadis assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CP/CPS. QuoVadis does not warrant that any third party's software will support or enforce such controls or requirements, and all Relying Parties are advised to seek appropriate technical or legal advice.

Parties relying on a Certificate must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of the associated Certificate against the relevant CRL or OCSP resource provided by QuoVadis. Relying on an unverifiable digital signature or SSL/TLS session may result in risks that the Relying Party assumes in whole and which QuoVadis does not assume in any way.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS;
- That the Certificate is being used in accordance with its key usage field extensions specified in this CP/CPS and contained in the Certificate; and
- That the Certificate is valid at the time of reliance by reference to the QuoVadis CRL or OCSP and the Certificate has not been revoked.

Warranties are only valid if the steps detailed above have been carried out.

#### **4.6. Certificate Renewal**

Renewal of a Certificate means reissuance of the Certificate using the same key pair. QuoVadis does not support Renewal; key pairs must always expire at the same time as the associated Certificate. QuoVadis makes reasonable efforts to notify Subscribers of the imminent expiration of a Certificate. Identification and Authentication procedures are generally the same for replacement Certificates as for a new application.

#### **4.7. Certificate Re-Key**

Re-keying a Certificate means to request a new Certificate with the same contents except for a new key pair. Identification and Authentication procedures are the same for re-key as for a new application.

#### **4.8. Certificate Modification**

QuoVadis may reissue or replace a valid Certificate when the Subscriber's common name, organization name, device name, or geographic location changes. Modified information must undergo the same Identification and Authentication procedures as for a new Certificate.

#### **4.9. Certificate Revocation And Suspension**

##### **4.9.1. Circumstances For Revocation**

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. QuoVadis may revoke any Certificate at its sole discretion or based on information confirmed in a Certificate Problem Report. QuoVadis will revoke a Certificate if:

- QuoVadis determines that any of the information appearing in the Certificate is not accurate;
- The Subscriber requests revocation of its Certificate;
- The Subscriber indicates that the original Certificate Request was not authorised and does not retroactively grant authorization;
- QuoVadis obtains reasonable evidence that there has been loss, theft, modification, unauthorised disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate;

- QuoVadis receives notice or otherwise becomes aware that a Subscriber has breached a material obligation under the Subscriber Agreement or other contractual obligations;
- QuoVadis receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
- QuoVadis receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew its domain name;
- QuoVadis determines, in its sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or QuoVadis' CP/CPS;
- QuoVadis receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Subscriber that is contained within the Certificate;
- If QuoVadis receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination;
- Either the Subscriber's or QuoVadis' obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- 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 appropriately authorised representatives can request revocation of a Certificate. QuoVadis may, if necessary, also confirm the revocation request by contact with additional, authorised representatives of the Subscriber.

Parties who are not the Subscriber (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 Subscriber, 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 where appropriate, may forward such complaints to law enforcement and/or revoke 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 revokes the Certificate and issues a new CRL as soon as it has determined that a properly supported revocation request has been made.

**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 3280.

QuoVadis updates and publishes a new CRL of revoked Certificates on a 12-hour basis or more frequently under special circumstances. The CRLs for Certificates issued pursuant to this CP/CPS can be accessed via the URLs contained in the Certificate Profile for that Certificate.

**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 support suspension of Certificates.

**4.9.14. Who Can Request Suspension**

The QuoVadis PKI does not support suspension of Certificates.

**4.9.15. Procedure For Suspension Request**

The QuoVadis PKI does not support suspension of Certificates.

**4.9.16. Limits On Suspension Period**

The QuoVadis PKI does not support suspension of Certificates.

**4.10. Certificate Status Services**

Not applicable.

**4.11. End Of Subscription**

A Subscriber 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 or recovery of Subscriber private keys.

**5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

The section of the CP/CPS provides a high level description of 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 biometric readers.

### **5.1.3. Power And Air-Conditioning**

All critical components are connected to uninterrupted power supply (UPS) units to prevent abnormal shutdown in the event of a power failure. Automatic failover to standby generators is provided.

### **5.1.4. Water Exposures**

The QuoVadis secure operating area provides protection against water. It is located on an upper floor with raised flooring, floors and walls are sealed, and the enclosure meets the requirements of DIN 18095.

### **5.1.5. Fire Prevention And Protection**

The QuoVadis secure operating area provides protection against fire according to DIN 4102 F90 with an automatic FM200 extinguishing system.

### **5.1.6. Media Storage**

All magnetic media containing QuoVadis PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the QuoVadis service operations area or in a secure off-site storage area.

### **5.1.7. Waste Disposal**

Paper documents and magnetic media containing QuoVadis PKI information or confidential information are securely disposed of by:

- in the case of magnetic media: physical damage to or complete destruction of the asset; or the use of an approved utility to wipe or overwrite magnetic media; or
- in the case of printed material, shredding or destruction by an approved service.

### **5.1.8. Off-Site Backup**

An offsite location is used for the storage and retention of backup software and data. The off site storage is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e. software and data are stored in fire-rated safes and containers which are located behind access-controlled doors in areas accessible only by authorised personnel).

## **5.2. Procedural Controls**

Administrative processes are described in detail in the various documents used within and supporting the QuoVadis PKI. Administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CP/CPS and other relevant operational documents. Except for certain RA functions described in this CP/CPS, QuoVadis does not outsource operations associated with Root CA2.

### **5.2.1. Trusted Roles**

In order to ensure that one person acting alone cannot circumvent security, trusted responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons are acting within the realms

of their responsibilities and within the stated security policy. This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of checks and balances to occur among the various roles.

#### **5.2.2. Number Of Persons Required Per Task**

At least two people are assigned to each trusted role to ensure adequate support at all times except verifying and reviewing audit logs. Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the PKI, most especially the Root CA and Issuing CA private keys.

CA key pair generation and initialisation of each CA (Root and Issuing) shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

#### **5.2.3. Identification And Authentication For Each Role**

Persons filling trusted roles must undergo an appropriate security screening procedure, designated "Position of Trust". Each individual performing any of the trusted roles shall use a Certificate stored on an approved cryptographic smart card to identify themselves to the Certificate Server and Repository.

#### **5.2.4. Roles Requiring Separation Of Duties**

Operations involving Root and Issuing CA roles are segregated between M of N employees. All operations involving maintenance of audit logs are segregated.

### **5.3. Personnel Controls**

#### **5.3.1. Qualifications, Experience, And Clearance Requirements**

Background checks are conducted on all individuals selected to take up a trusted role in the QuoVadis PKI in accordance with a designated security screening procedure, prior to the commencement of their duties.

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) 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 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 a Issuing CA private key. This plan includes procedures for:

- Revoking all Certificates signed with that Issuing CA's private key;
- Promptly notifying all Subscribers 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 succeeding entities. Before terminating its own CA activities, QuoVadis will where possible take the following steps:

- Give timely notice of revocation to each affected Subscriber.
- Revoke all Certificates that are still un-revoked or un-expired at the end of the notice period without seeking Subscriber's consent.
- Make reasonable arrangements to preserve its records according to this CP/CPS.
- Reserve its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary standards.
- Notify relevant government and accreditation bodies under applicable laws and related regulations or standards.

Upon termination of a CA, QuoVadis personnel shall destroy the CA private key by deleting, overwriting, or physical destruction.

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1. Key Pair Generation And Installation**

#### **6.1.1. Key Pair Generation**

CA private keys are protected within cryptographic modules that are validated to FIPS 140-2 Level-3. Access to the modules within the QuoVadis environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple members of the QuoVadis management team. Such allocation ensures that no one member of the team holds total control over any component of the system.

#### **6.1.2. Private Key Delivery To Certificate Holder**

Subscribers are solely responsible for the generation of the private keys used in their Certificate Requests unless specifically agreed by QuoVadis. QuoVadis does not provide SSL key generation, escrow, recovery or backup facilities.

#### **6.1.3. Public Key Delivery To Certificate Issuer**

Upon making a Certificate Application, the Subscriber is solely responsible for generating an RSA key pair and submitting it to QuoVadis in the form of a PKCS#10 CSR. Certificate requests are generated using the key generation facilities available in the Subscriber's web server software.

#### **6.1.4. Certification Authority Public Key To Relying Parties**

QuoVadis public keys are securely delivered to software providers to serve as trust anchors in commercial browsers and operating system root stores, or may be specified in a Certificate validation or path discovery policy file. Relying Parties may also obtain QuoVadis self-signed CA Certificates containing its public key from the QuoVadis web site.

#### **6.1.5. Key Sizes**

Key lengths within the QuoVadis PKI are determined by Certificate Profiles more fully disclosed in Appendix A and Appendix B. The QuoVadis Issuing CA uses an RSA minimum key length of 2,048 bit modulus. Subscribers may submit 1024-bit or 2048-bit keys to QuoVadis.

#### **6.1.6. Public Key Parameters Generation And Quality Checking**

The cryptographic modules used by QuoVadis have been validated to conforming to FIPS 140-2 Level-3 and provide random number generation and on-board creation of suitable key lengths for RSA public key generation.

#### **6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field)**

QuoVadis CA Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and also to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of QuoVadis. Key usages are specified in the Certificate Profiles in Appendix A and B.

### **6.2. Private Key Protection And Cryptographic Module Engineering Controls**

#### **6.2.1. Cryptographic Module Standards And Controls**

The cryptographic modules used by the QuoVadis PKI are validated to provide FIPS 140-2 Level-3 security standards in both the generation and the maintenance in all Root and Issuing CA private keys.

#### **6.2.2. Private Key (N Out Of M) Multi-Person Control**

Subject to the requirements of the CP/CPS, the QuoVadis PKI uses trusted multi-person control for both access control and authorisation control.

#### **6.2.3. Private Key Escrow**

Private keys shall not be escrowed.

#### **6.2.4. Private Key Backup**

Issuing CA private keys are stored in an encrypted state (using an encryption key to create a "cryptographic wrapper" around the key. Access is only by N-of-M control as defined in this CP/CPS. Backup copies are maintained on site and in secure, offsite storage.

#### **6.2.5. Private Key Archive**

The QuoVadis PKI does not support private key archive.

**6.2.6. Private Key Transfer Into Or From A Cryptographic Module**

See Section 6.2.4.

**6.2.7. Private Key Storage On Cryptographic Module**

See Section 6.2.4.

**6.2.8. Method Of Activating Private Key**

An authorised user must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

Subscribers are solely responsible for protection of their private keys. QuoVadis maintains no involvement in the generation, protection, or distribution of such keys. QuoVadis suggests that Subscribers use a strong password or equivalent authentication method to prevent unauthorised access and usage of the Subscriber private key.

**6.2.9. Method Of Deactivating Private Key**

Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorised access. After use, they must be deactivated using, for example, a manual logout procedure or a passive timeout. When not in use, cryptographic modules should be removed and securely stored, unless they are within the sole control of an authorised user.

Subscribers should also deactivate their private keys via logout and removal procedures when they are not in use.

**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 Issuing CAs have established an approved System Security Policy that incorporates computer security technical requirements that are specific to QuoVadis and configured to allow the minimal amount of connectivity identified as being necessary to accomplish CA functions.

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 and Procedures that include but are not limited to:

- Access controls to CA services and PKI roles;
- Enforced separation of duties for CA Services and PKI roles;
- Identification and Authentication of personnel that fulfil roles of responsibility in the QuoVadis PKI;
- Use of cryptography for session communication and database security;
- Archive of CA history and audit data;
- Use of cryptographic smart cards and x.509 Certificates for all administrators.

#### **6.5.2.      *Computer Security Rating***

The QuoVadis approved System 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.

#### **6.6.3.      *Life Cycle Security Controls***

QuoVadis employs a configuration management methodology for the installation and ongoing maintenance of the CA systems. The CA software, when first loaded, provides a method for QuoVadis to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

The QuoVadis Chief Security Officer periodically verifies the integrity of the CA software and monitors the configuration of the CA systems.

#### **6.6.4. Network Security Controls**

All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

All unused network ports and services on Issuing CA equipment are turned off to provide protection against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone (offline) configurations.

#### **6.6.5. Hardware Cryptographic Module Engineering Controls**

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

#### **6.7. Time-Stamping**

See Section 5.5.5.

### **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 follow the ITU X.509v3 standard, which allows a CA to add certain Certificate extensions to the basic Certificate structure. QuoVadis uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

##### **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 Constraints**

See Appendix A and Appendix B.

##### **7.1.6. Certificate Policy Object Identifier**

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a CP/CPS such as this. The Certificate Policy OIDs that incorporate this CP/CPS into a given Certificate by reference (and identify that this CP/CPS applies to a given Certificate containing the OID) are listed in Appendix A and Appendix B.

##### **7.1.7. Usage Of Policy Constraints Extension**

Not applicable.

##### **7.1.8. Policy Qualifiers Syntax And Semantics**

QuoVadis Certificates include a brief statement in the Policy Qualifier field of the Certificate Policy extension to inform potential Relying Parties on notice of the limitations of liability and other terms and conditions on the use of the Certificate, including those contained in this CP/CPS, which are incorporated by reference into the Certificate.

##### **7.1.9. Processing Semantics For The Critical Certificate Policies Extension**

No stipulation.

## **7.2. CRL Profile**

### **7.2.1. *Version Number***

QuoVadis issues version 2 CRLs conforming to RFC 3280, and which contain the basic fields listed below:

Version  
Issuer Signature Algorithm  
Issuer Distinguished Name  
thisUpdate (UTC format)  
nextUpdate (UTC format – thisUpdate plus 12 hours)  
Revoked Certificates list  
Serial Number  
Revocation Date (see CRL entry extension for Reason Code below)  
Issuer's Signature

### **7.2.2. *CRL And CRL Entry Extensions***

CRL Number (monotonically increasing integer - never repeated)  
Authority Key Identifier (same as Authority Key Identifier in Certificates issued by CA)

#### *CRL Entry Extensions*

Invalidity Date (UTC - optional)  
Reason Code (optional)

## **7.3. Online Certificate Status Protocol Profile**

OCSPP is enabled for all Certificates within the QuoVadis PKI.

### **7.3.1. *Online Certificate Status Protocol Version Numbers***

OCSPP 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 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 controls service quality by performing ongoing internal audits against a randomly selected sample of Certificates. In addition, QuoVadis conducts audits of LRAs to verify their compliance with this CP/CPS and applicable service agreements.

**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, including periodic audits.

**9.2.2. No Partnership or Agency**

Subscriber 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 Subscriber 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**

Subscribers 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)

### **9.3.2. Information Not Within The Scope Of Confidential Information**

Information appearing in Certificates or stored in the Repository is considered public and not within the scope of confidential information, unless statutes or special agreements so dictate.

## **9.4. Responsibility To Protect Private Information**

All Participants in the QuoVadis PKI QuoVadis and all others using or accessing any personal data in connection with matters dealt with this CP/CPS shall comply with the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amending and/or implementing legislation enacted from time to time, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. QuoVadis complies with the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

### **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. Third Party LRA Representations and Warranties**

Third party LRAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to, or which reasonably ought to be known to, the LRA or its agents;
- There are no errors in the information in the Certificate that were introduced by the LRA or its agents as a result of a failure to exercise reasonable care; and
- Their Certificates meet all material requirements of this CP/CPS.

Additional representations and warranties relevant to LRAs may be included in Subscriber Agreements for specific Certificate Policies.

**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 authorised 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 unauthorised use and that no unauthorised person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to QuoVadis regarding the information contained in the Certificate are accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify QuoVadis of any material inaccuracies contained in the Certificate.
- The Certificate is used exclusively for authorised and legal purposes, consistent with this CP/CPS, and that the Subscriber will use the Certificate only in conjunction with the entity named in the organisation field of the Certificate.
- The Subscriber agrees with the terms and conditions of this CP/CPS and other agreements and policy statements of QuoVadis.

### **9.6.3. Relying Parties Representations And Warranties**

The Relying Party is solely responsible for making the decision to rely on a QuoVadis Certificate. A Relying Party accepts that in order to reasonably rely on a QuoVadis Certificate, the Relying Party must:

- Read and agree with the terms of the QuoVadis Relying Party Agreement including the limitations of liability for reliance on a QuoVadis Certificate
- Verify the QuoVadis Certificate by referring to the relevant CRL in the QuoVadis Repository and trust the Certificate only if it is valid and has not been revoked or has expired.
- Rely on a QuoVadis Certificate only as may be reasonable under the circumstances, given (i) the Relying Party's previous course of dealing with the Subscriber, (ii) the economic value of the transaction or communication, (iii) the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the transaction or communication, (iv) all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CP/CPS, and (v) any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the communication or transaction.

### **9.6.4. Representations And Warranties Of Other Participants**

Not applicable.

### **9.7. Disclaimers Of Warranties**

QuoVadis disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as

cannot be excluded at law. In no event and under no circumstances (except for fraud or wilful misconduct) shall QuoVadis be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages;
- Any costs, expenses, or loss of profits;
- Any death or personal injury;
- Any loss of data;
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates or digital signatures;
- Any other transactions or services offered within the framework of this CP/CPS;
- Any other damages except for those due to reliance, on the information featured on a Certificate, or on the verified information in a Certificate;
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or wilful misconduct of the Applicant or Subscriber;
- Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this CP/CPS;
- Any liability that arises from the usage of a Certificate that is not valid;
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CP/CPS;
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses; or
- Any liability that arises from compromise of a Subscriber's private key.

#### **9.8. QuoVadis Liability**

QuoVadis shall be liable to Subscribers or Relying Parties for direct loss arising from any breach of this CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to \$5000 per Subscriber or Relying Party per Certificate. QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this Certificate Policy & Certification Practice Statement, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

##### **9.8.1. Limitations of Liability**

QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis' liability to any person for damages arising under, out of or related in any way to this CP/CPS, Subscriber Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. QuoVadis shall 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 PKI (including, without limitation, the use of or reliance upon Certificates), any person that participates within the QuoVadis PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon the foregoing as a condition and inducement to permit that person to participate within the QuoVadis Public Key Infrastructure.

##### **9.8.2. Exclusions of Liability**

QuoVadis shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorised disclosure or unauthorised use of the Certificate or any password or activation data used to control access thereto;
- If the Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or organisation;
- If the Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this QuoVadis CP/CPS and/or the relevant Subscriber Agreement or any applicable law or regulation;
- If the private key associated with the Certificate held by the claiming party or otherwise the subject of any claim has been compromised;
- If the Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that QuoVadis uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided QuoVadis uses commercially reasonable methods to protect against such disturbances;
- 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, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which QuoVadis is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of QuoVadis.

### **9.9. Indemnities**

Any user of a QuoVadis Certificate, whether a Subscriber, Relying Party or otherwise, shall indemnify and hold harmless QuoVadis from any and all damages and losses arising out of: (i) use of the QuoVadis Certificate in a manner not authorised by QuoVadis; (ii) tampering with the QuoVadis Certificate; or (iii) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional. In addition, Subscribers shall indemnify and hold harmless QuoVadis from any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a QuoVadis Certificate relating to: (i) Subscriber's breach of its obligations under the Subscriber Agreement or this CP/CPS; (ii) Subscriber's failure to protect its private key; or (iii) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by Subscriber.

### **9.10. Term And Termination**

#### **9.10.1. Term**

This CP/CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

#### **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 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 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 Subscriber 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 Subscriber Agreement for the Certificate in question.

**9.15. Compliance With Applicable Law**

Subscribers 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**

Any provision of this QuoVadis CP/CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this QuoVadis CP/CPS or affecting the validity or enforceability of such remaining provisions.

**9.16.5. Enforcement (Waiver Of Rights)**

Except where an express time frame is set forth in this CP/CPS, no delay or omission by QuoVadis to exercise any right, remedy, or power it has under this CP/CPS shall impair or be construed as a waiver of such right, remedy, or power. A waiver by QuoVadis of any breach or covenant in this CP/CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. No waiver shall be effective unless it is in writing. Bilateral agreements between QuoVadis and the parties to this CP/CPS may contain additional provisions governing enforcement.

**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.



## 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
Cert Hash(sha1):	ca 3a fb cf 12 40 36 4b 44 b2 16 20 88 80 48 39 19 93 7c f7

## 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: <a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a>
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 = <a href="http://ocsp.quovadisglobal.com">http://ocsp.quovadisglobal.com</a>
CRL Distribution Points	c = no; CRL HTTP URL = <a href="http://crl.quovadisglobal.com/QVRCA2.crl">http://crl.quovadisglobal.com/QVRCA2.crl</a>
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):	3b c2 6d b5 fb 5e bb 57 05 aa 7a 5d b9 39 44 e3 66 8e 12 7d

**Appendix B – Subscriber Certificate Profiles****Business SSL**

<b>Field</b>	<b>Value</b>
Version	V3
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, 2, or 3 years expressed in UTC format
<b>Subject Distinguished Name</b>	
Organization Name	subject:organisationName (2.5.4.10 )
Organisation Unit	subject:organisationUnit (2.5.6.5) Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)
Country	subject:countryName (2.5.4.6)
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)
<b>Extension</b>	<b>Value</b>
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; Digital Signature, Key Encipherment (a0)
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)

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: <a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a> [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 = <a href="http://ocsp.quovadisglobal.com">http://ocsp.quovadisglobal.com</a>
CRL Distribution Points	c = no; CRL HTTP URL = <a href="http://crl.quovadisglobal.com/QVSSLICA.crl">http://crl.quovadisglobal.com/QVSSLICA.crl</a>

### ***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 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 Subscribers***

Individuals (natural persons), incorporated entities, government entities, general partnerships, unincorporated associations, and sole proprietorships may be Subscribers 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 Subscriber 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 the services of a third party to confirm Applicant information. QuoVadis accepts confirmation from third party organisations, other third party databases, and government entities.

***Application Process***

During the Certificate approval process, QuoVadis Validation Specialists employ controls to validate the identity of the Applicant and other information featured in the Certificate Application to ensure compliance with this CP/CPS.

Step 1: The Applicant provides a signed Certificate Application to QuoVadis, which includes identifying information to assist QuoVadis in processing the request and issuing the Business SSL Certificate, along with a PKCS#10 CSR and billing details.

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

Step 3: The Applicant accepts the Subscriber Agreement and approves Certificate issuance.

Step 4: All signatures are verified through follow-up procedures or telephone calls.

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 Business SSL Certificate.

Step 7: The Business SSL Certificate is delivered to the Applicant.

***Renewal***

Renewal requirements and procedures include verification that the Applicant continues to have authority to use the domain name, and that the Certificate Application is approved by an authorised representative of the Applicant.

**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	
<b>Subject Distinguished Name</b>		
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 3280, 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:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 3280 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 3280 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 3280 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 'V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)' or 'V1.0, Clause 5.(d)', 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)	
<b>Extension</b>	<b>Value</b>	
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; Digital Signature, Key Encipherment (a0)	
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
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: <a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a> [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 = <a href="http://ocsp.quovadisglobal.com">http://ocsp.quovadisglobal.com</a>	
CRL Distribution Points	c = no; CRL HTTP URL = <a href="http://crl.quovadisglobal.com/QVSSLICA.crl">http://crl.quovadisglobal.com/QVSSLICA.crl</a>	

**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 behaviour 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 the Issuance and Management of 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 Organizations, Government Entities, and Business Entities satisfying the requirements specified below:

**(a) Private Organization Subjects**

- The Private Organization MUST be a legally recognised entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation (e.g., by issuance of a Certificate of Incorporation) or is an entity that is chartered by a state or federal regulatory agency;
- The Private Organization MUST have designated with the Incorporating Agency either 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 an equivalent facility;
- The Private Organization MUST have a verifiable physical existence and business presence.
- The Private Organization's Jurisdiction of Incorporation, Registration, Charter, or License 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 Bermuda; and
- The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda.

**(b) Government Entity Subjects**

- The legal existence of the Government Entity MUST be established by the political subdivision in which it operates;
- The Government Entity MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a Certificate by the laws of Bermuda; and
- The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda.

**(c) Business Entity Subjects**

Business Entities are entities that do not qualify as Private Organizations as defined in subsection (a) but do satisfy the following requirements. Business Entities may include general partnerships, unincorporated associations, sole proprietorships, and individuals (natural persons).

- The Business Entity MUST be a legally recognised entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, Certificate, or license, and whose existence can be verified with that Registration Agency;
- The Business Entity MUST have a verifiable physical existence and business presence;
- At least one Principal Individual associated with the Business Entity MUST be identified and validated;
- The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;
- Where the Business Entity represents itself under an assumed name, QuoVadis MUST verify the Business Entity's use of the assumed name;
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where QuoVadis is prohibited from doing business or issuing a Certificate under the laws of Bermuda; and
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be listed on any government denial list or prohibited list (such as a trade embargo) under the laws of Bermuda.

**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 or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named

in the EV Certificate legally exists as a valid organisation or entity in the Jurisdiction of Incorporation or Registration;

- Identity: QuoVadis has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: QuoVadis has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;
- Authorization for EV Certificate: QuoVadis has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorised the issuance of the EV Certificate;
- Accuracy of Information: QuoVadis has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- 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 organisation 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 (business presence at a physical address), and
  - Verify Applicant's operational existence (business activity).
- ii. Verify Applicant (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV Certificate;
- iii. Verify Applicant's authorization for the EV Certificate, including;
  - Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
  - Verify that Contract Signer signed the Subscriber Agreement; and
  - Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

The vetting regime of the EV Guidelines includes detailed verification procedures, which vary by Subscriber, and may include direct confirmation with Incorporating Agencies as well as correlation of information from certain qualified commercial data providers, site visits, and independent confirmations from senior officers of the Applicant. Verified opinion letters from attorneys and accountants representing the Applicant, as well as bank account verifications, may also be used to fulfil aspects of the vetting process.

### ***Applicant Contacts***

The EV Guidelines specify a number of Applicant roles involved in the EV verification process. All must be filled by natural persons (i.e., specific individuals as opposed to generic titles or automated systems). The Applicant may appoint one individual to fill all these roles, separate individuals for each role, or more than one person for any role.

QuoVadis requires Applicants for EV Certificates to execute an EV Authority Letter to identify and authorise the various Applicant contacts, as well as to enable the use of online confirmations and approvals for various aspects of the EV process.

- Certificate Requester: The initial contact that submits the Certificate Application to QV on behalf of the Applicant. This person does NOT need to be an employee of the Applicant, but must be an authorised agent with express authority to represent the Applicant. Certificate Requesters are formally recognised by QuoVadis only after QuoVadis has confirmed their appointment with the Applicant.
- Certificate Approver: MUST be an employee of the Applicant with express authority to represent the Applicant to (a) act as a Certificate Requester and to authorise other employees or third parties to act as a Certificate Requester, and (b) to approve EV Certificate Requests submitted by other Certificate Requesters.
- Contract Signer: MUST be an employee of the Applicant with express authority to sign Subscriber Agreements on behalf of the Applicant.
- Confirming Person: Must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) able to sign the QV Authority Letter on behalf of the Applicant.

### ***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 a domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorised 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 organisation 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 Authority Letter from the Applicant is already in its possession). Alternate procedures may also be used to authenticate the identity and authority of individuals involved in the Certificate Application.

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.

Step 9: The EV Certificate is delivered to the Certificate Requester.

QuoVadis may not issue an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that QuoVadis knows, or by the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the EV Certificate Request and notify the Applicant accordingly.

### ***Renewal***

Under the EV Guidelines, renewal requirements and procedures are generally the same as those employed for the validation and issuance for new Applicants. The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is one year, except for the identity and authority of individuals identified in the EV Authority Letter.

In the case of outdated information, QuoVadis repeats the verification processes required by the EV Guidelines. If a company is no longer in good standing, or if any of the other required information cannot be verified, the Certificate is not renewed.