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

/5..D40Cep0O76 h4Rs [- Tc -1P ,bg

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:

Table of Contents

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

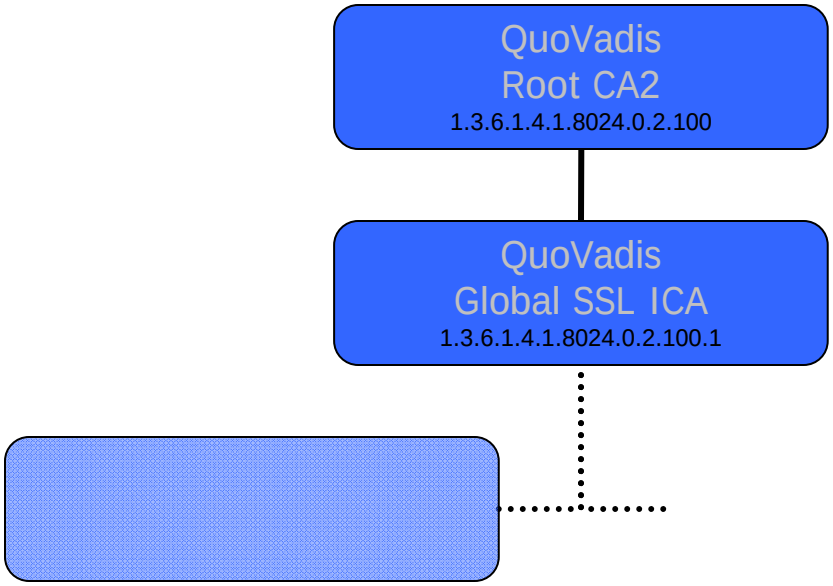
Participants (Participants) within the QuoVadis PKI include:

- 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

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.

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

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 conducthat thSigning Ration of Organisation

QuoVadis, in its sole discretion, may

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;
-

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

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

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

5.3.4. Retraining Frequency And Requirements

Validation Specialists engaged in Certificate validation and issuance must maintain adequate skill levels in order to

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

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

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

- Originated from the software developer;

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 ofsRecord beiof

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 T ertificates and

- 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

- 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

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

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.

QuoVadis Global SSL ICA

Field	Value
Version	V3

Appendix B – Subscriber Certificate Profiles

Business SSL

Field	Value
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
Subject Distinguished Name	
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)
Extension	**Value**
Authority Key Identifier	c=no; Octet String – Same as Issuer's 32 4d a1 4f ea f0 ae 99 b6 ee 9b 07 2c 84 08 11 50 8b e2 7e
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	c=yes; 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: http://www.quovadisglobal.com/cps [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 2 Certification Policies and Certificate Practice Statement.
Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =http://ocsp.quovadisglobal.com
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/QVSSLICA.crl

Purposes of Business SSL

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

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

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

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	

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		

Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)	

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

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[(Ap5.1 -1 Tf1s))3(is a(e g)4.8(stems

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.

-

Step 2: QuoVadis independently verifies