1. INTRODUCTION

1.1. Overview

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

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

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that QuoVadis Root CA2 uses in the generation, issue, use, and management 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 three forms of Certificates according to the terms of this CP/CPS:

i. Business SSL Certificates 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 Certificates are Certificates issued in compliance with 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.

iii. Trusted Code Signing Certificates are Certificates issued in compliance with Microsoft’s Code Signing Certificate Guidelines, including identification of the certificate subject by a verified organization name and certificate revocation for any misrepresentation or publication of malicious code.

QuoVadis Certificates comply with Internet standards (x509 v.3) as set out in RFC 5280 (which supersedes 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.

The diagram below illustrates the components of the QuoVadis PKI:

1.3.2. Registration Authorities

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

Office Address:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11, Bermuda
Email: compliance@quovadisglobal.com

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.

Application Software Vendors: Mean those developers of Internet browser software or other software that displays or uses certificates and distribute Root Certification Authority Certificates embedded in their software, including but not limited to KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, Red Hat, Inc., Adobe, etc.

Authority Letter: The Authority Letter is a signed by a Confirming Person acting for the Applicant for EV 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.

must identify the legal entity that intends to have control over the use of the Private Key when signing code. 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

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

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsibl

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 orig

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

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

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

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

4.9.5. Time Within Which The CA Must Process The Revocation Request
QuoVadis will take commercially reasonable steps to revoke the Digital Certificate within 4 hours of receipt of a valid revocation request.

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

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

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

4.9.8. Maximum Latency For CRL
The maximum latency for the CRL is 10 minutes.

4.9.9. On-Line Revocation/Status Checking Availability
QuoVadis provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of the Certificate.

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

4.9.11. Other Forms Of Revocation Advertisements Available
Not applicable.

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

4.9.13. Circumstances For Suspension
The QuoVadis PKI does not 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.

- 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 dural naa((e accessTD(Admino[0dre)] Tw 0.0676 Tw 27.267 0w 00 9 72 656.7001 Tts, .7001 Tt-27.267 -1 Tf0.001 Tc 3.806

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.

- 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

- 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

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

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

e1(a)39(t)42(e)41(a)39(r)41(c)D 2 >

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 5280, 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
OCSP is enabled for all Certificates within the QuoVadis PKI.

7.3.1. Online Certificate Status Protocol Version Numbers
OCSP Version 1, as defined by RFC 2560, is supported within the QuoVadis PKI.

7.3.2. Online Certificate Status Protocol Extensions
No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1. Frequency, Circumstance And Standards Of Assessment
The practices specified in this CP/CPS have been designed to meet or exceed the requirements of, and QuoVadis is audited for compliance to, generally accepted and developing industry standards including:

- AICPA/CICA WebTrust for Certification Authorities and the WebTrust Extended Validation Program;
- Bermuda Authorised Certification Service Provider standards of the Bermuda electronic Transactions Act;
- Swiss Zert ES Qualified Certification Service 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

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.

- 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;
-

- Read and agree with the terms of the QuoVadis Relying Party Agreement including the limitations on the usage of the Certificate and also 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

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

QuoVadis Global SSL ICA

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

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

Purposes of Business SSL

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

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

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

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

Eligible 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 **a(8e Ca 8s4Dts**

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.

Extended Validation SSL

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

State/Province of Incorporation	

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

Purpose of EV SSL

EV SSL Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL

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;

k2[illegible]--k0o00ipe[illegible]snl9Tw8disl4format[illegible]snl9Tw8disl4format

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.

Trusted Code Signing

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 Trusted Code 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
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	c=yes; Digital Signature (80)
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codeSigning)
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.2.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 2 Certification Policies and Certificate Practice Statement.

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/QVTCSICA.crl

Purposes of Trusted Code Signing

The primary purpose of QuoVadis Trusted Code Signing Certificates is to establish that executable code originates from a source identified by QuoVadis. 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 Trusted Code Signing Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to sign code in the name to be included in the Certificate 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 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 Trusted Code Signing Certificate.

Step 7: The Certificate is delivered to the Applicant.

Renewal

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