Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement herein after referred to as the CP/CPS adopted by QuoVadis Limited (QuoVadis). The QuoVadis CP/CPS contains an overview of the practices and procedures that QuoVadis employs for its operation as a Digital Certification Authority. This document is not intended to create contractual relationships between QuoVadis Limited and any other person. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business. This version of the CP/CPS has been approved for use by the QuoVadis Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA and as otherwise set out herein. The date on which this version of the CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

Contact Information:

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

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

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

Version Control:

Table of Contents

1. INTRODUCTION

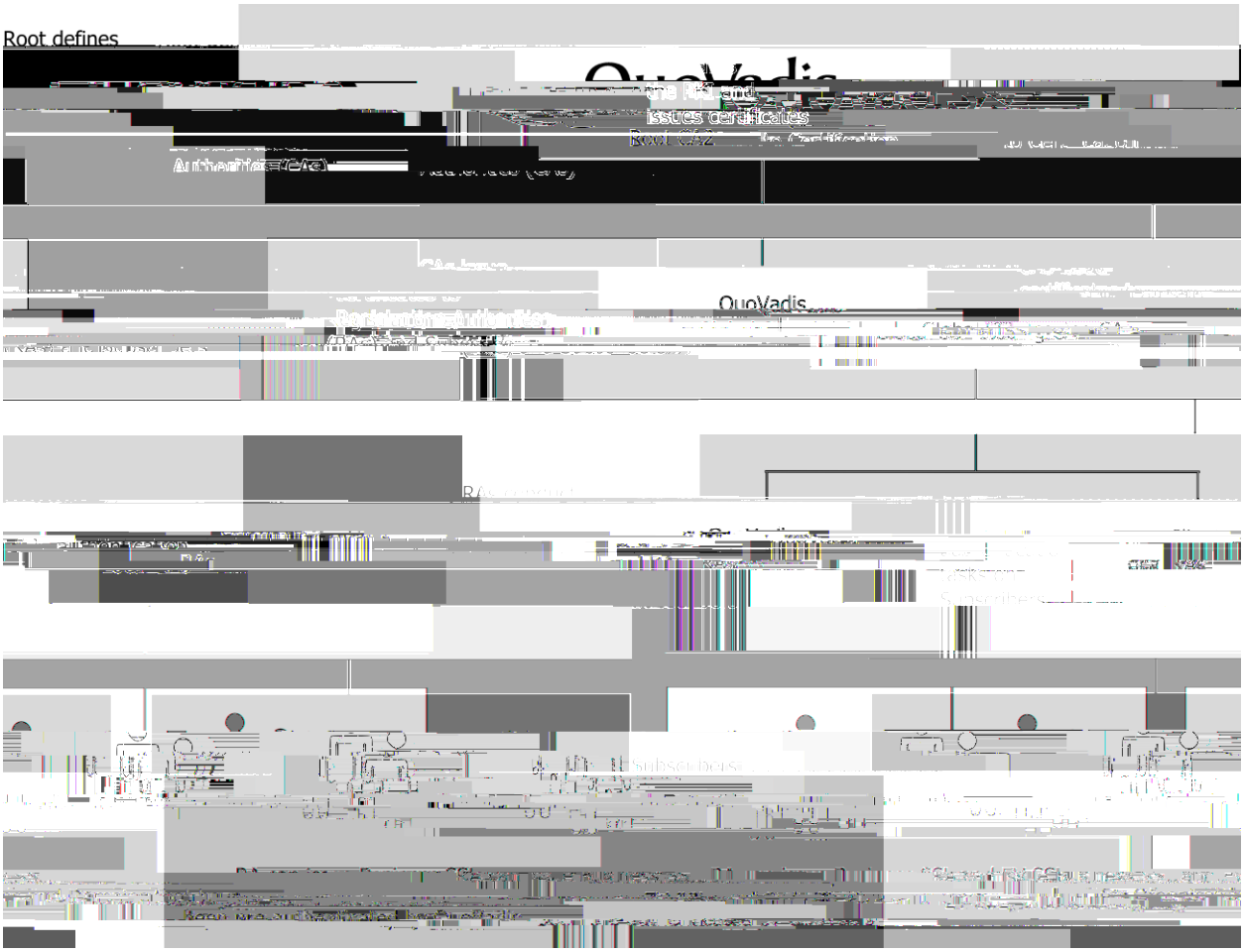
1.1. Overview

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

QuoVadis Code Signing Certificates are used to provide users with reasonable assurance that the executable code

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

The diagram below illustrates the components of the QuoVadis PKI:



1.3.1. Certification Authority

The following OIDs are pertinent to this CP/CPS:

QuoVadis Root CA2/ QuoVadis Root CA 2 G3	1.3.6.1.4.1.8024.0.2
QuoVadis Global SSL ICA/ QuoVadis Global SSL ICA G3	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

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 Certificate Holder information in accordance with this CP/CPS;
- Revoke Certificates upon receipt of a valid request from an authorised person

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

3.1.4. Rules For Interpreting Various Name Forms

QuoVadis to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

3.1.8. High Risk Domains

QuoVadis maintains a list of High Risk Domains and has implemented technical controls to prevent the issuance of Certificates to certain domains. QuoVadis follows documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval.

3.2. Initial Identity Validation

3.2.1. Method To Prove Possession Of Private Key

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

3.2.2. Authentication Of Organisation Identity

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

3.2.3. Authentication Of Individual Identity

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

3.2.4. Non-Verified Certificate Holder Information

QuoVadis does not verify information contained in the Organisation Unit (OU) field in Certificates. Other information may be designated as non-verified in specific Certificate Profiles.

3.2.5. Validation Of Authority

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

4.2.2. Approval Or Rejection Of Certificate Applications

From time to time, QuoVadis may modify the requirements related to application information requested, based on QuoVadis requirements, business context of the usage of Certificates, or as may be required by law, changes to the EV Guidelines or changes to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

QuoVadis, in its sole discretion, may refuse to accept an application for a Certificate or for the renewal of a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. Qu

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

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The section of the CP/CPS provides a high level description of the security policy, physical aROLS

5.2.1. Trusted Roles

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

5.2.2. Number Of Persons Required Per Task

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

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

5.2.3. Identification And Authentication For Each Role

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

5.2.4. Roles Requiring Separation Of Duties

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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, And Clearance Requirements

5.3.3. Training Requirements

QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and

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 certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by

..08 Tm[ )]TJETBT33.30624.11 0 00098[O(mi-t)157.5a)]di sTJ739noJEt 0-72(p)6(((C-t)y)5(id(uo)e)6(TJ739S57.5S57.5L)]3(973(k)5(e)6(y)]3(973(g)6(

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

Computer security technical requirements are achieved utilising a combination of hardened security modules and software, operating system security features, PKI and CA software and physical safeguards, including security Policies and Procedures that include but are not limited to:

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

6.5.1. Computer Security Rating
A version of the core Certificate Authority software used by QuoVadis has obtained the globally recognised Common Criteria EAL 4+ certification.

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

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

6.6.1. System Development Controls
Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and 1d 1dnETBT1(ftw)ydwclosc1.

6.7 Network Security Controls

All access to Issuing CA

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 Certificate Holder'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 Certificate Holder obligations stated in this CP/CPS, Certificate Holders 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 Certificate Holder represents to QuoVadis and to Relying Parties that at the time of

- 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 Certificate Holder;
- 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;
-

- If the private key associated with the Certificate held by the claiming party or otherwise the subject of any claim has been compromised;
-

9.10.3. Effect Of Termination And Survival

The conditions and effect resulting from termination of this CP/CPS will be communicated via the QuoVadis website upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The re

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 ï Root and Issuing CA Profiles

QuoVadis Root CA2

Field	Value
Version	V3
Serial Number	Unique number 0509
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	25 years expressed in UTC format NotBefore: 11/24/2006

QuoVadis Global SSL ICA

Field	Value
Version	V3
Serial Number	Unique number 057a
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 1/12/2007 16:13:33 NotAfter: 1/12/2017 16:13:11
Subject Distinguished Name	

QuoVadis Global SSL ICA G3

Field	Value
Version	V3
Serial Number	Unique number 7ed6e79cc9ad81c4c8193ef95d4428770e341317
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 G3 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 11/6/2012 14:50:18 NotAfter: 11/6/2022 14:50:18
Subject Distinguished Name	CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256RSA {1.2.840.113549.1.1.11 }
Extension	Value
Authority Key Identifier	c=no; KeyID= ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d
Subject Key Identifier	c=no; b3 12 89 b5 a9 4b 35 bc 15 00 f0 80 e9 d8 78 87 f1 13 7c 76
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	c=no; Certificate Policies; {All issuance policies }
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=1
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/qvrca2g3.crl
Key Id Hash(sha1):	9a e2 98 4b 15 27 e9 9c f7 71 45 2b 27 d1 0e 5e dc 36 d5 41
Cert Hash(sha1):	e9 0b cc a3 d1 34 12 7e f6 46 e8 54 72 3f 13 7d 79 71 db 64

Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)
Authority Information Access	c=no; Access Method= - Id-

QuoVadis Root CA2 C0C0ers0RC11QyrighA2Vadis RoLRmitd:ooPub8(l9(R)9(Rc)8(o))3(D)-3( )8(c)8(um)124entC]TJE04 .04 2.024 742

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) or sha256RSA (1.2.840.113549.1.1.11)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Global SSL ICA or CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	
Validity Period	1 or 2 years	

Commitment to Comply with Guidelines

QuoVadis conforms to the current version of the CA/Browser Forum "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guideline

- The International Organization Entity MUST NOT be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at a domain name listed on the EV Certificate, and to use the EV Certificate solel09lel(te)7 9e at

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.

Code Signing

Field	Value	Comments
Version	V3	
Serial Number	Unique number	
Issuer Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	
Issuer Distinguished Name	CN = QuoVadis Code Signing CA G1 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)	Required field. The Subject's verified legal name.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Optional field. Must not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless QuoVadis has verified this information
Common Name	subject:commonName (2.5.4.3)	Required field. The Subject's verified legal name.
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	Required if the subject:localityName field is absent. Optional if the subject:localityName fields is present.
Locality	subject:locality (2.5.4.6)	Required if the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field is present.
Country	subject:countryName (2.5.4.6)	Required field.
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Issuer's Signature	sha256RSA (1.2.840.113549.1.1.11)	
Extension	Value	
Authority Key Identifier	c=no; Octet String	
Subject Key Identifier	c=no; Octet String	
Key Usage	c=yes; Digital Signature (80)	
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codeSigning)	

3. Obtains a biometric associated with the Subject, such as a fingerprint or notarized handwritten Declaration of Identity,
4. Verifies the Certificate Requester's authority to request a certificate and the authenticity of the Certificate request using a verified method of communication.

A Declaration of Identity is a written document that consists of the following:

1. the identity of the person performing the verification,
2. a signed declaration by the verifying person stating that they verified the identity of the Applicant,
3. a unique identifying number from an identification document of the verifier,
4. a unique identifying number from an identification document of the Applicant,
5. the date and time of the verification, and
6. a declaration of identity by the Applicant that is signed in handwriting in the presence of the person performing the verification.

Application Process