QUOVADIS ROOT CA2
CERTIFICATE POLICY /

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 p

- 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/	

QuoVt CA1 T.45TJ 0 Tc01C(s)-8(10)10(V)-e(ba)-1Ayelyt CA 1.3.6.1.4.1.80240.2

Confirming Person: A confirming Person is a natural person who must be a senior officer of tho mi musio(-2( )e.-2( )f be

3.1.5. Uniqueness Of Names

such refusal. QuoVadis reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3. Time To Process Certificate Applications

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

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

4.3. Certificate Issuance

- QuoVadis determines, in its sole discretion, that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
- If QuoVadis receives notice or otherwise becomes aware that a Certificate Holder has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination;
- Either the Certificate Holder's or QuoVadis' obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- A QuoVadis CA Private Key used to issue that Certificate has been compromised;
- Revocation is required by the QuoVadis CP/CPS
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
- QuoVadis' right to issue and manage Certificates under the EV Guidelines or the Baseline Requirements expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository); or
- QuoVadis ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

4.9.2. Who Can Request Revocation

QuoVadis may revoke any Certificate issued within the QuoVadis PKI at its sole discretion. The Certificate Holder and its appropriately authorised representatives can request revocation of a Certificate. QuoVadis may, if necessary, also confirm the revocation request by contact with additional, authorised representatives of the Certificate Holder.

Parties who are not the Certificate Holder (such as Relying Parties, Application Software Vendors, and other third parties) may file a Certificate Problem Report to initiate a Certificate revocation request. Problem reports may include complaints; suspected private key compromise or Certificate misuse; or other types of fraud, compromise, misuse, or inappropriate conduct related to the Certificate.

tf5S Tc S 9 JaTc 0 Tw 3.91(P)-5 Ih5(h)-8(91(P)-5 Ih 3-5 728 93(r8 Tm73 4.)90(9.)90(3. ET /ID Qe)5S Tc S 9 J [(t)-7t)-5 .32 0

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-L On [(fo)-yabcu6 Tw re W n BT CS0 CS 0 9(d)1(O)20n BTtw 2 T-5(C)1d ifP m4 Tm e1 1 Tt(lit)

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) shall1(i)-4(n) 0 Tw 0 -1.2138-6(o)-g1(i)-4(de)-13(qu)liaaspec a lo

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 trusted roles.

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

prTrm TJdd-dslis.

upon request of any of the entities involved in the transaction or their

6.4.3. Other Aspects Of Activation Data

No stipulation.

6.5. Computer Security Controls

- Any business continuity, incident response, contingency, and disaster recovery plans;
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information;
- Any information held by QuoVadis as private information in accordance with Section 9.4;
- Any transactional, audit log, and archive records including Certificate Application records and documentation submitted in support of Certificate Applications whether successful or rejected; and
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS)

9.3.2. Information Not Within The Scope Of Confidential Information

Information appearing in Certificates or stored in the Repository is considered public and not within( )1(w)-11(i)-4(t)-5ed pud any

reserves the right to revoke a Certificate at any time and at its sole discretion. Private keys and public keys are the property of the applicable Certificate Holders who rightfully issue and hold them.

This QuoVadis CP/CPS and the P

- 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

9.10.3. Effect Of Termination And Survival

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

9.11. Individual Notices And Communications With Participants

Electronic mail, postal mail, fax, and web pages will all be valid means of QuoVadis providing any of the notices required by this CP/CPS, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid means of providing any notice required pursuant to this CP/CPS to QuoVadis unless specifically provided otherwise (for example in respect of revocation procedures).

9.12. Amendments

9.12.1. unlessu0 Tc 22.52.533 0 esSubcedure For Amendment

Amendments to this CP/CPS are made and approved by the QuoVadis Policy Management Authority (PMA). Amendments shall be in the form of an amended CP/CPS or a replacement CP/CPS. Updated versions of this CP/CPS supersede any designated or conflicting provisions of the referenced version of the CP/CPS.

9.12.2. unlessu0 T8 Tc -0.097 0 essNotification Mechanism And Period

The QuoVadis PMA reserves the right to amend this CP/CPS without notification for amendments that are not material, including typographical corrections, changes to URLs, and designate amendments as material or non-material is a

9.12.3. unlessu0 T4 Tc -0.093 0 essCircumstances unlessu0 T4 Tc -0.093 0 essMust Be Changed

Unless the QuoVadis PMA determines otherwise, the OID for this CP/CPS shall not change. If a change in QuoVadis' certification practices is determined by the PMA to warrant a change in the currently specified OID for a particular Certificate Policy, then the revised version of this CP/CPS will also contain a revised OID for that Certificate Policy.

QuoVadis Root CA 2 G3

Field	Value
Version	V3
Serial Number	Unique number 445734245b81899b35f2ceb82b3b5ba726f07528
Issuer Signature	

Appendix B – Certificate Holder Certificate Profiles

Business SSL

Field	Value
Version	V3
Serial Number	

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

State/Province of Incorporation	subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	ASN.1 - X520StateOrProvinceName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above.
Country of Incorporation	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)	ASN.1 - X520countryName as specified in RFC 5280 Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code.
Registration Number	Subject:serialNumber (2.5.4.5)	For Private Organisations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number

Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10

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

- 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
- The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Subsidiary organizations or agencies of qualified International Organizations may also qualify for EV Certificates issued in accordance with the EV Guidelines.

Additional Warranties and Representations for EV Certificates

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

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

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

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 Certificate Holder 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 Certificate Holder, 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

ode Signing

Field	Value	Comments
Version	V3	
Serial Number	Unique number	
Issuer Signature Algorithm	sha256RSA (	

Field	Value	Comments
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; {2.23.140.1.2.3} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository	1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID. 1the Quo-1(di)-17(sTw 8.28 0627 0 Td (.04

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

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 in accordance with the "Verification Requirements" section above.

Step 3: The Applicant accepts the Certificate Holder 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-4(l)-eces saralls.