QuoVadis Root CA 2 / QuoVadis Root CA 2 G3

Certification Policy / Certification Practice Statement

OIDs: 1.3.6.1.4.1.8024.0.2

Effective Date: August 25, 2020

Version: 2.9

Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited (QuoVadis), a company of

Version Control

Author	Date	Version	Comment
QuoVadis PMA			

QuoVadis PMA	27 March, 2020	2.8	Changes to comply with Mozilla Root Store Policy v2.7, CA/B Forum Ballot SC25, revised Subscriber Agreement and Terms of Use, and changes to reflect policies and practices adopted from, and editorial conformity with, DigiCert where applicable.
QuoVadis PMA	25 August, 2020	2.9	Updates to domain validation and CAA methods. Reduction in TLS validity period. Update to revocation services information.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

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. The term "QuoVadis Root CA2" applies to all generations of this Root.

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 four forms of Certificates according to the terms of this CP/CPS:

i) Business SSL Certificates are Organisation Validated (OV) Certificates for which limited authentication and authorisation checks are performed on the Subscriber and the individuals acting for the Subscriber.

ii) Extended Validation SSL Certificates are issued in compliance with the 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) Qualified Website Authentication Certificates (QWAC) (QCP-w) are issued in compliance with Regulation (EU) No. 910/2014 on electronic identification and trustt7(2)4.3(0)-1.7(1)4.3(4)it7(2uoMdk1e)-4.9e.2(ing

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 Object Identifier (OID) assigned to QuoVadis Root CA2/ QuoVadis Root CA 2 G3 is 1.3.6.1.4.1.8024.0.2.

Separate policy documents in the QuoVadis Repository apply to QuoVadis Certificates signed by the following Root CAs:

- QuoVadis Root Certification Authority/QuoVadis Root CA 1 G3 (OID 1.3.6.1.4.1.8024.0.1) and

- Revoke Certificates upon receipt of a valid request from an authorised person or on its own initiative when circumstances warrant; and
- Notify Subscribers of the imminent expiry of their Certificates.

Issuing CAs chaining to a QuoVadis Root must not be used for Man in the Middle (MITM) purposes or for the traffic management of domain names or IP addresses that the entity does not own or control.

Issuing CAs chaining to a publicly trusted QuoVadis Root must either be technically constrained, or undergo an independent audit and be publicly disclosed in the Repository on the QuoVadis website (https://www.quovadisglobal.com/repository).

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 Enterprise Registration Authorities (ERAs) and authorise the issuance of TLS/SSL Certificates by QuoVadis for Organisations and Domains that have been vetted by QuoVadis and pre-authenticated by QuoVadis. ERAs must abide by all the requirements of this CP/CPS and the terms of their services agreement with QuoVadis. ERAs may also implement more restrictive practices based on their internal requirements. QuoVadis does not delegate authority to third party RAs to vet TLS/SSL certificate contents.

The QuoVadis Portal is a secure web application that facilitates RAs' activities as well as the ongoing management of the TLS/SSL Certificates for which they are responsible.

1.3.3. Subscribers

In the context of this CP/CPS, the Subscriber is the Individual responsible for requesting, installing and maintaining the trusted system for which a TLS/SSL Certificate has been issued. 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

1.4. CERTIFICATE USAGE

1.5.4. 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. See also Section 9.10 and Section 9.12.

1.6. DEFINITIONS AND ACRONYMS

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

Application Software Vendors: Means a software developer whose software displays or uses QuoVadis Certificates and distributes QuoVadis' Root Certificates.

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.

Authorisation Number: A unique identifier of a Payment Service Provider acting as the Subscriber for PSD2 Certificates. The Authorisation Number is used and recognized by the NCA.

Authorisation Domain

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.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA. A Random Value is specified by QuoVadis and exhibits at least 112 bits of entropy.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA. Also known as Issuing CA.

Subscriber: Means either the Individual to whom an end entity Certificate is issued or the Individual responsible for requesting, installing and maintaining the trusted system for which an TLS/SSL Certificate has been issued.

Subscriber Agreement: Is the agreement executed between a Subscriber and QuoVadis relating to the provision of designated Certificate-related services that governs the Subscriber's rights and obligations related to the Certificate.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Acronyms

AND	Authorisation Domain Name
ALPN	TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737
CA	Certificate Authority or Certification Authority
CAA	Certificate Authority Authorisation
CP/CPS	Certificate Policy & Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
eIDAS	Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market
ETSI	European Telecommunications Standards Initiative
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
ERA	Enterprise Registration Authority
LRA	Local Registration Authority

PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PMA	QuoVadis Policy Management Authority
Portal	Certificate Management System
PSD2	Payment Services Directive - Directive (EU) 2015/2366

3. IDENTIFICATION AND AUTHENTICATION

The Identification and Authentication procedures used by QuoVadis depend on the Class of Certificate being issued. See Appendix B for Certificate Profiles and the relevant verification requirements.

3.1. NAMING

3.1.1. Types Of Names

All Subscribers require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). TLS/SSL Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service, or application that has been confirmed with the Subscriber. The Distinguished Names of a Code Signing Certificate must identify the legal entity that intends to have control over the use of the Private Key when signing code. The Baseline Requirements prohibit Certificates containing Internal Server Names or Reserved IP Addresses.

Wildcard TLS/SSL Certificates have a wildcard asterisk character for the server name in the Subject field. Wildcard EV Certificates may not be issued under the EV Guidelines.

The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and the Subject Alternative Name extension.

3.1.2. Need For Names To Be Meaningful

QuoVadis uses Distinguished Names that identify both the entity (i.e. person, organisation, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. QuoVadis only allows directory information trees that accurately reflect organisation structures.

3.1.3. Pseudonymous Subscribers

QuoVadis does not issue anonymous or pseudonymous Certificates under this CP/CPS for Internationalised Domain Names (IDN), QuoVadis may include the Punycode version of the IDN as a Subject Name

3.1.4. Rules For Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness Of Names

The Subject Name of each Certificate issued by an Issuing CA shall be unique within each class of Certificate issued by that Issuing CA over the lifetime of that Issuing CA and shall conform to applicable X.500 standards for the uniqueness of names.

The Issuing CA may, if necessary, insert additional numbers or letters to the Subscriber's Subject Common Name, or other attribute such as subject serialNumber, in order to distinguish between two Certificates that would otherwise have the same Subject Name. Name uniqueness is not violated when multiple Certificates are issued to the same entity.

3.1.6. Recognition, Authentication, And Role Of Trademarks

Unless otherwise specifically stated in this CP/CPS, Qu

3.2.1. Method To Prove Possession Of Private Key

Issuing CAs shall establish that each Applicant for a Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the request for a Certificate. The Issuing CA shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol, including PKCS#10. 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.

3.2.2.1. Validation of Domain Authorisation and Control

For each FQDN listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

i) Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation)

ii) Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorisation Domain Name (ADN). Performed in accordance with BR section 3.2.2.4.4;

iii) Confirming the Applicant's control over the requested ADN (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value in a DNS record. Performed in accordance with BR section 3.2.2.4.7;

iv) Confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8;

v) Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12;

vi) Confirming the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact and then receiving a confirming response utilizing the Random Value. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance w2.th BR Section 3.2.2.4.13;

vii)

and a confirming response is provided for each domain. Performed in accordance with BR Section 3.2.2.4.17;

xi) Confirming the Applicant's control over the requested FQDN by confirming the presence of an agreed-upon Random Value under the "/.well-known/pki-validation" directory. Performed in accordance with BR section 3.2.2.4.18; and

xii) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method, performed in accordance with BR Section 3.2.2.4.19. This method is suitable for validating Wildcard Domain Names; or

xiii) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the ALPN Extension, performed in accordance with BR Section 3.2.2.4.20. This method is NOT suitable for validating Wildcard Domain Names.

QuoVadis verifies an Applicant's or Organisation's right to use or control of an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following:

i) By verifying domain control over the email Domain Name using one of the procedures listed in this section; or

ii) by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response within a limited period of time that includes the Random Value to indicate that the Applicant controls that same email address.

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.

3.2.2.2. Authentication for an IP Address

For each IP Address listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

i) Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;

ii)

3.3.2. Identification and Authentication For Re-Key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial Identification and Authentication process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

See Section 4.9 for information about Certificate Revocation procedures. All revocation requests are authenticated by QuoVadis or the RA responsible for issuing the Certificate.

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit A Certificate Application

The process to apply for QuoVadis Certificates varies by Certificate Policy and is described in Appendix B. Either the Applicant or an individual authorised to request Certificates on behalf of the Applicant may submit Certificate Requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to QuoVadis

QuoVadis does not issue Certificates to entities on a government denied list maintained by the United States or that are located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrolment Process And Responsibilities

Certificate Requests must be in a form prescribed by the Issuing CA and typically include i) an application form including all registration information as described by this CP/CPS, ii) secure generation of KeyPair and delivery of the Public Key to QuoVadis, iii) acceptance of the relevant Subscriber Agreement or other terms of use upon which the Certificate is to be issued, iv) and payment of fees. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

All agreements concerning the use of, or reliance upon, Certificates issued within the QuoVadis PKI must incorporate by reference the requirements of this QuoVadis CP/CPS as it may be amended from time to time.

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 required by the Certificate Application to ensure compliance with this CP/CPS.

QuoVadis considers a source's availability, purpose, and reputation when determining whether a third-party data source is reasonably reliable. For TLS/SSL QuoVadis does not consider a database, source, or form of identification reasonably reliable if QuoVadis or the RA is the sole source of the information.

4.2.2. Approval Or Rejection Of Certificate Applications

After receiving a Certificate Application, QuoVadis or an RA verifies the application information and other information in accordance with this CP/CPS.

If an RA (including an Enterprise RA) assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks. After verification is complete, QuoVadis Validation Specialists evaluate the corpus of information and decides whether or not to approve issuance.

Approval for EV requires two QuoVadis Validation Specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsible for installing the issued Certificate on the Subscriber's computer or cryptographic module according to the Subscriber's system specifications. A Subscriber is deemed to have accepted a Certificate when:

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

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

4.4.2. Publication Of The Certificate By The CA

QuoVadis publishes all CA Certificates in its Repository. QuoVadis publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3. Notification Of Certificate Issuance By The CA To Other Entities

Issuing CAs and RAs within the QuoVadis PKI may choose to notify other entities of Certificate issuance.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key And Certificate Usage

The Certificate shall be used lawfully in accordance with the QuoVadis CP/CPS and Subscriber Agreement.

Subscribers are obligated to protect their Private Keys from unauthorised use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key And Certificate Usage

A Party seeking to rely on a Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement. Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. QuoVadis does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by QuoVadis are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the QuoVadis Repository.

A Relying Party should rely on a digital signature or TLS/SSL handshake only if:

i) the Digital Signature or TLS/SSL session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,

ii) the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and

iii) the Certificate is being used for its intended purpose and in accordance with this CP/CPS.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance For Certificate Renewal

QuoVadis may renew a Certificate if:

i) the associated Public Key has not reached the end of its validity period;

ii)

4.7.2. Who May Request Re-Key

QuoVadis will accept re-key requests from the Subject of the Certificate, an authorised representative for an Organisational certificate, or the nominating RA. QuoVadis may initiate a certificate re-key at the request of the Certificate Subject or at QuoVadis' own discretion.

4.7.3. Processing Certificate Re-Key Request

Certificate re-key requests are processed in the same manner as requests for new Certificates and in accordance with the provisions of this CP/CPS. In order to process a re-key request, the Subscriber is required to:

i) Confirm that details contained in the original Certificate application have not changed; and

ii) Authenticate their identity to the RA.

4.7.4. Notification of Certificate Re-Key To Subscriber

QuoVadis may deliver the Certificate in any secure fashion, such as using a QuoVadis Portal.

4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate

Conduct constituting acceptance of a re-keyed Certificate is in accordance with section 4.4.1Issued Certificates are considered accepted 30 days after the Certificate is re-keyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.7.6. Publication of The Re-Key Certificate By The CA

QuoVadis publishes a re-keyed Certificate by delivering it to the Subscriber.

4.7.7. Notification of Certificate Re-Key By The CA To Other Entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances For Certificate Modification

Modifying a Certificate means creating a new Certificate for the same Subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP/CPS. The new Certificate may have the same or a different subject Public KeyModified information must undergo the same Identification and Authentication procedures as for a new Certificate.

4.8.2. Who May Request Certificate Modification

QuoVadis modifies Certificates at the request of certain Certificate Subjects or in its own discretion. QuoVadis does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, QuoVadis verifies any information that will change in the modified Certificate. QuoVadis will only issue the modified Certificate after completing the verification process on all modified informationRAs are required to perform Identification and Authentication of all modified Subscriber information in accordance with the requirements of the applicable Certificate Profile.

4.8.4. Notification Of Certificate Modification To Subscriber

QuoVadis may deliver the Certificate in any secure fashion, such as using a QuoVadis Portal.

viii) QuoVadis confirms that the Certificate was not issued in accordance with the CA/B forum requirements or relevant browser policy;

ix) QuoVadis determines or confirms that any of the information appearing in the Certificate is

v) QuoVadis confirms that the CA Certificate was not issued in accordance with or that Issuing CA has not complied with the CP/CPS;

vi) QuoVadis determines that any of the information appearing in the CA Certificate is inaccurate or misleading;

vii) QuoVadis or the Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;

viii) QuoVadis' or the Issuing CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless QuoVadis has made arrangements to continue maintaining the CRL/OCSP Repository;

ix) Revocation is required by the QuoVadis CP/CPS; or

x) The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Vendors or Relying Parties.

4.9.2. Who Can Request Revocation

Any appropriately authorised party, such as a recognised representative of a Subscriber or RA, may request revocation of a Certificate. QuoVadis may revoke a Certificate without receiving a request and without reason. Third parties may request Certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

QuoVadis provides Anti-Malware Organisations, Subscribers, Relying Parties, Application Software Vendors, and other third parties (such as a National Competent Authority that issued the Authorisation Number in a PSD2 Certificate) with clear instructions on how

In the case of a PSD2 Certificate, the NCA identified in the Certificate may request revocation by contacting psd2@quovadisglobal.nl. NCA revocation requests are authenticated using either a previously communicated shared secret, or use of a digital signature supported by Qualified Certificate issued to the NCA.

QuoVadis maintains a continuous 24x7 ability to internally respond to high priority revocation requests. Subscribers may also revoke their Certificates via the QuoVadis Portal.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. 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 revoke a CA Certificate within one hour after receiving clear instructions from the PMA.

Within 24 hours after receiving a Certificate problem report, QuoVadis investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

4.9.6. Revocation Checking Requirement For Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the Certificate path in accordance with IETF PKIX standards, including checking for Certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7. CRL Issuance Frequency

QuoVadis uses its offline Root CAs to publish CRLs for its Issuing CAs at least every 6 months and within 18 hours after revoking an Issuing CA Certificate. QuoVadis updates the CRL for end-user Certificates at least every 12 hours and the date of the “Next Update” field will not be more than 3 calendar days after the date in the field “Effective Date”. A CRL is valid for a maximum of 72 hours.

Before revoking an Issuing CA Certificate a last CRL is generated with a nextUpdate field value of "99991231235959Z”. QuoVadis does not issue a last CRL until all Certificates in the scope of the CRL are either expired or revoked.

After the expiry date of an Issuing CA the most recent CRL will be published for at least 1 month. QuoVadis does not use the ExpiredCertsOnCRL extension.

4.9.8. Maximum For Relying

QuoVadis supports an OCSP capability using the GET method for Certificates. OCSP Responders under QuoVadis' direct control will not resp

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Archival Escrow And Recovery Policy And Practices

This CP/CPS does not support key escrow or recovery of Subscriber Private Keys.

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

Not applicable.

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. QuoVadis maintains a security program to:

i) Protect the confidentiality, integrity, and availability of data and business process;

ii) Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of data and business process;

iii) Protect against unauthorised or unlawful access, use, disclosure, alteration, or destruction of data and business process;

iv) Protect against accidental loss or destruction of, or damage to data and business processes; and

v) Comply with all other security requirements applicable to the CA by law and industry best practices.

QuoVadis performs an annual risk assessment to identify internal and external threats and assess likelihood and potential impact of these threats to data and business processes.

5.1. PHYSICAL CONTROLS

QuoVadis manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with CA operations.

5.1.1. Site Location and Construction

QuoVadis performs its CA and TSA operations from secure datacentres located in Bermuda, the Netherlands, and Switzerland. The datacentres are equipped with logical and physical controls that make QuoVadis' CA and TSA operations inaccessible to non-trusted personnel. QuoVadis operates under a security policy designed to detect, deter, and prevent unauthorised access to QuoVadis's operations.

5.1.2. Physical Access

QuoVadis permits entry to its secure datacentre only to security-cleared and authorised personnel, whose movements within the facility are logged and audited. A police background check forms part of the security clearance authorisation process. Physical access is controlled by dual-factor authentication using a combination of physical access cards and biometric readers.

5.1.3. Power And Air-Conditioning

Datacentres have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power

5.1.5. Media Storage

5.2.1.6. Security Officers

The Security Officer is responsible for administering and implementing security practices.

5.2.2. Number Of Persons Required Per Task

QuoVadis requires that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating QuoVadis' Private Keys, generating a CA Key Pair, or backing up a QuoVadis Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification And Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure commensurate to their roleAll personnel are required to authenticate themselves to CA, TSA, and RA systems before they are

5.3.3. Training Requirements

QuoVadis provides relevant skills training in QuoVadis' PKI and TSA operations for the personnel performing verification duties including:

- basic PKI knowledge,
- software versions used by QuoVadis,
- authentication and verification policies and procedures,
- QuoVadis security principles and mechanisms,
- disaster recovery and business continuity procedures,
- common threats to the validation process, including phishing and other social engineering tactics, and
- CA/Browser Forum Guidelines and other applicable industry and government guidelines.

QuoVadis maintains records of who received training. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of such Certificates. Where competence is demonstrated in lieu of training, QuoVadis maintains supporting documentation.

5.3.4. Retraining Frequency And Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. QuoVadis makes employees acting in trusted roles aware of any changes to QuoVadis' operations as necessary for them to perform their role. If QuoVadis' operations change, QuoVadis will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency And Sequence

Not applicable.

5.3.6. Sanctions For Unauthorised Actions

QuoVadis employees and agents failing to comply with this CP/CPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and
rete,

- CA and Subscriber Certificate lifecycle management events;
- Security events, including
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

QuoVadis event logs include:

- Date and time of the entry
- Serial or sequence number of entry (for automatic journal entries)
- Details of the of entry (name, type etc)
- Source of entry (for example, terminal, port, location, customer, IP address)
- Destination address (if relevant)
- identity of the entity making the journal entry (e.g. User ID)

5.4.2. Frequency Of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3. Retention Period For Audit Log

QuoVadis audit logs are retained for at least seven (7) years. Certain high volume system generated logs are retained for 18 months based on a risk assessment.

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 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 Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures

Each Issuing CA performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing CA premises and storage at a secure, offsite location.

5.4.6. Audit Collection System

The security audit process of each Issuing CA runs independently of the Issuing CA software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7. Notification To Event-Causing Subject

Where an event is logged, no notice is required to be given to the individual, organisation, device, or application that caused the event.

5.4.8. Vulnerability Assessment

QuoVadis performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any

certificate data or certificate issuance process. QuoVadis also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that QuoVadis has in place to control such risks. QuoVadis' Internal Auditors review the security audit data checks for continuity. QuoVadis' audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

5.5.1. Types Of Records Archived

QuoVadis archives and makes available upon authorised request documentation subject to the QuoVadis Document Access Policy. For each Certificate, the records will address creation, issuance, use, revocation, expiration, and renewal activities. These records will include all relevant evidence in the Issuing CA's possession including:

- Audit logs;
- Certificate Requests and all related actions;
- Evidence produced in verification of Applicant details;
- Contents of issued Certificates;
- Evidence of Certificate acceptance and signed (electronically or otherwise) Subscriber Agreements;
- Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- CRLs posted; and
- Audit Opinions as discussed in this QuoVadis CP/CPS.

5.5.2. Retention Period For Archive

Audit logs relating to the certificate lifecycle are retained as archive records for a period of for seven (7) years. Detailed system generated logs are retained for 18 months based on a risk assessment.

5.5.3 Of

5.5.6. Archive Collection System

The QuoVadis Archive Collection System is internal.

5.5.7. Procedures To Obtain And Verify Archive Information

Only specific QuoVadis Trusted Roles and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their authorised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.6. KEYCHANGEOVER

Key changeover is not automatic but procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, QuoVadis ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, QuoVadis im

6.1.4. CA Public Key To Relying Parties

QuoVadis' Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root stores, and/or as roots signed by other CAs. All accreditation authorities supporting QuoVadis Certificates and all application software providers are permitted to redistribute QuoVadis root anchors.

QuoVadis may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may also obtain QuoVadis CA Certificates from QuoVadis' web site or by email.

6.1.5. Key Sizes

QuoVadis follows the relevant ETSI and NIST guidance in using and retiring signature algorithms and key sizes. Key sizes for individual Certificate Profiles are disclosed in Appendix A and Appendix B. Currently QuoVadis generates and uses at least the following key sizes, signature algorithms and hash algorithms for signing Certificates, CRLs and OCSP responses:

- 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8);
- 256-bit ECDSA Key or greater with the matching Secure Hash Algorithm version as required; or
- a hash algorithm that is equally or more resistant to a collision attack allowed by the references in sections 1.1 and 8.1.

QuoVadis requires end-entity Certificates to contain a key siqej.9(e)-1.1( )5.9atus tadi ioarifier Hel(ri)3l(ri)3mhorg (ed)5.2( )52

Qu55.4(ada)-4.(A an58.4(d)5Sub.cribm vhm)6..mh(n)2y fulatu(n)2i9(almm)]TJ8743108 0 TD.3001 Tc-.9001 TwSP rsesisis.6(

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1.

this CP/CPS. QuoVadis will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

QuoVadis personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CA/B Forum's Network Security Requirements.

6.4.2. Activation Data Protection

If activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module. PINs may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the PIN. Activation Data should be memorised, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Subscriber's personal information.

6.4.3. Other Aspects Of Activation Data

Where a PIN is used, the User is required to enter the PIN and identification details such as their Distinguished Name before they are able to access and install their Keys and Certificates.

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.

6.5.1. Specific Computer Security Technical Requirements

QuoVadis secures its CA systems and authenticates and protects communications between its systems and trusted roles. QuoVadis' CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

RAs must ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

QuoVadis' CA systems are configured to:

i) authenticate the identity of users before permitting access to the system or applications;

ii)

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

QuoVadis has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. QuoVadis only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by QuoVadis are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to QuoVadis' operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

QuoVadis has mechanisms in place to control and continuously monitor the security-related configurations of its CA systems. When loading software onto a CA system, QuoVadis verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

QuoVadis CA and RA functions are performed using networks secured in accordance to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

QuoVadis documents and controls the configuration of its systems, including any upgrades or modifications made. Root Keys are kept offline and brought online only when necessary to sign Issuing CA Certificates,

7. CERTIFICATE,

7.1.7. Usage Of Policy

7.2.

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:

WebTrust	WebTrust Principles and Criteria for CAs WebTrust Principles and Criteria for CAs – SSL Baseline with Network Security WebTrust Principles and Criteria for CAs – Extended Validation SSL WebTrust Principles and Criteria for CAs – Publicly Trusted Code Signing Certificates
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
ETSI EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates
ETSI EN 319 412-1	

8.4. TOPICS COVERED BY ASSESSMENT

Audits as applicable cover QuoVadis' business practices disclosure, the integrity of QuoVadis' PKI operations, and an Issuing CAs' compliance with this CP/CPS and referenced requirements. Audits verify that QuoVadis is compliant with the CP/CPS and applicable standards and regulatory requirements.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to QuoVadis' services, then (i) the auditor will document the discrepancy, (ii) the auditor will promptly notify QuoVadis, and (iii) QuoVadis will develop a plan to cure the noncompliance. QuoVadis will submit the plan to the PMA for approval and to any third party that QuoVadis is legally obligated to satisfy. The PMA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. QuoVadis is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the PMA to address the non-compliant Issuing CA.

8.6. PUBLICATION OF AUDIT RESULTS

The results of each audit are reported to the PMA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. The results of the most recent audits of QuoVadis are posted at https://www.quovadisglobal.com/accreditations.

8.7. SELF-AUDITS

QuoVadis controls service quality by performing quarterly self-audits against a randomly selected sample of TLS/SSL Certificates being no less than three percent of the Certificates issued. Audits of other Certificate types will be at the discretion of QuoVadis to gain reasonable assurance of compliance to applicable requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance

9.1.5. Refu

QuoVadis may esta nd policy, details of which may b in relevant contractual agreements.

9.2. FINAN PONSIBILITIES

9.2.1. Ins overage

QuoVadis maintai wing insurance related to its respect nce and obligations:

- Comm al Liability insurance (occurrenc olicy limits of at least $2 million in cove
- Professio Errors & Omissions ins limits of at least $5 million in coverage, a erage for (i) cl ar g out of an act, error, or omission, un ject r maintaining EV Certificates, and (ii) claims fo igemen prietary rights of any third party (excluding copy rk infringem vasion of privacy and advertising injury.

9.2.2. Other Assets

No stipulation.

9.2.3. Insu Warranty Coverage Fo tities

Subscribers are entitl commercial insuran or financial protection agai accidental occurrences ons insura.1(lvida)-3.7(r)

Other End d

9.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

9.4.1. Privacy Plan

QuoVadis follows the Privacy Notices posted on its website when handling personal information. See https://www.quovadisglobal.com/Privacy. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9.4.2. Information Treated As Private

Personal information about an individual that is not publicly available in the contents of a Certificate or CRL is considered private. QuoVadis protects private information using appropriate safeguards and a reasonable degree of care.

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

QuoVadis employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. QuoVadis will not divulge any private Subscriber information to any third party for any reason, unless compelled to do so by law or competent regulatory authority. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice And Consent To Use Private Information

In the course of accepting a Certificate, individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the QuoVadis CA, and used as explained in the

9.5.2. Property Rights in the CP/CPS

Issuing CAs acknowledge that QuoVadis retains all intellectual property rights in and to this CP/CPS.

9.5.3. Property Rights in Names

A Subscriber and/or Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate and Distinguished Name within any Certificate issued to such Subscriber or Applicant.

9.5.4. Property Rights in Keys and Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of QuoVadis and end-user Subscribers that are the respective subjects of the Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these Key Pairs. Without limiting the generality of the foregoing, QuoVadis Root Public Keys and the Root CA Certificates containing them, including all Public Keys and self-signed Certificates, are the property of QuoVadis. QuoVadis licenses software and hardware manufacturers to reproduce such Root CA Certificates to place copies in trustworthy hardware devices or software.

9.5.5. Violation of Property Rights

Issuing CAs shall not knowingly violate the intellectual property rights of any third party.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. Certification Authority Representations

By issuing a Digital Certificate, QuoVadis represents and warrants that, during the period when the Digital Certificate is valid, QuoVadis has complied with this CP/CPS in issuing and managing the Digital Certificate to the parties listed below:

- The party to the relevant QuoVadis Subscriber Agreement and Terms of Use;
- All Relying Parties who reasonably rely on a Valid Certificate; and
- All Application Software Vendors with whom QuoVadis has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendor.

QuoVadis discharges its obligations by:

- QuoVadis complies, in all material aspects, with this CP/CPS, and all applicable laws and regulations;
- QuoVadis publishes and updates CRLs and OCSP responses on a regular basis;
- All Certificates issued under this CP/CPS will be verified in accordance with this CP/CPS and meet the minimum requirements found herein and in the Baseline Requirements; and
- QuoVadis will maintain a repository of public information on its website.

QuoVadis hereby warrants (i) it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue (ii) Certificates shall be revoked if QuoVadis believes or is notified

i) The RA's certificate issuance and management services conform to the QuoVadis CP/CPS and applicable CA or RA Agreements;

ii) Information provided by the RA does not contain any false or misleading information;

iii) Reasonable steps are taken to verify that the inform

i) Obtained sufficient knowledge on the use of Certificates and PKI;

ii) Studied the applicable limitations on the usage of Certificates and agrees to QuoVadis' limitations on liability related to the use of Certificates;

iii) Has read, understands, and agrees to the QuoVadis Relying Party Agreement and this CP/CPS;

iv) Verified both the Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP;

v) Will not use a Certificate if the Certificate has expired or been revoked; and

vi) Will take all reasonable steps to minimize the risk associated with relying on a Digital Signature, including only relying on a Certificate after considering:

   a. applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

   b. the intended use of the Certificate as listed in the Certificate or this CP/CPS;

   c. the data listed in the Certificate;

   d. the economic value of the transaction or communication;

   e. the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication;

   f. the Relying Party's previous course of dealing with the Subscriber;

   g. the Relying Party's understanding of trade, including experience with computer-based methods of trade; and

   h. any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorised reliance on a Certificate is at a party's own risk.

Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations And Warranties Of Other Participants

Participants within the QuoVadis PKI represent and warrant that they accept and will perform any and all duties and obligations as specified by this CP/CPS.

9.7. DISCLAIMERS OF WARRANTIES

OTHER THAN AS PROVIDED IN SECTION 9.6.1, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, QUOVADIS DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. QUOVADIS DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE. QuoVadis does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time. Subscriber's sole remedy for a defect in the Certificates is for QuoVadis to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that QuoVadis has no obligation to correct defects that arise

ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) QUOVADIS AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "QUOVADIS ENTITIES") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF; AND (B) THE QUOVADIS ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS CP/CPS OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO QUOVADIS IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER QUOVADIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CP/CPS, MAY BE MADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER.

For EU Qualified Certificates, QuoVadis liability is in

9.10.2. Termination

This CP/CPS as amended from time to time shall remain in force until it is replaced by a newer version.

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

QuoVadis accepts notices related to this CP/CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from QuoVadis. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. QuoVadis may allow other forms of notice in its Subscriber Agreements.

9.12. AMENDMENTS

9.12.1. Procedure For Amendment

Amendments to this CP/CPS are made and approved by the QuoVadis PMA at at least annually. Amendments are made by posting an updated version of the CP/CPS to the Repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS. Controls are in place to reasonably ensure that this CP/CPS is not amended and published without the prior authorisation of the QuoVadis PMA

9.12.2. Notification Mechanism And Period

QuoVadis posts CP/CPS revisions to the Repository (https://www.quovadisglobal.com/repository). QuoVadis does not guarantee or set a notice-and-comment period and may make changes to this CP/CPS without notice and without changing the version number. The QuoVadis PMA is responsible for determining what constitutes a material change of the CP/CPS.

9.12.3. Circumstances Under Which OID Must Be Changed

The QuoVadis PMA is solely responsible for determining whether an amendment to the CP/CPS requires an

Customer is Domiciled in:	Governing Law is laws of:	Court or arbitration body with exclusive jurisdiction:
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne
A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

9.15. COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5, QuoVadis meets the requirements of the European data protection laws and has established appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

QuoVadis contractually obligates each RA to comply with this CP/CPS and applicable industry guidelines. QuoVadis also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP/CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall

10. APPENDIX A – ROOT 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}

QuoVadis Root CA 2 G3

Field	Value
Version	V3
Serial Number	Unique number 445734245b81899b35f2ceb82b3b5ba726f07528

11. APPENDIX B

11.1. BUSINESS SSL

Field	Value

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/<CA Name>.crl

Purposes

Verification of Country: QuoVadis verifies the country associated with the Subject using one of the following:

i) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;

ii) the ccTLD of the requested Domain Name;

iii) information provided by the Domain Name Registrar; or

iv) a method identified in "Identity" above.

Application Process

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

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

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

Step 3: The Applicant accepts the Subscriber Agreement and approves Certificate issuance. Step 4: All signatures are verified through follow-up procedures or telephone calls.

Step 5: QuoVadis obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the Certificate Request and not4.7(nctv5623.0n ar)7ua not4(8(t)4.0008)4.y2 e :aeAD-.0dt008fingly.04 oedse :a tust

11.2. EXTENDED VALIDATION SSL

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique system generated random number assigned to each certificate, containing at least 64 bits of output.	
Issuer Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = Variable O = QuoVadis Limited C = BM	
Validity Period	1 or 2 years expressed in UTC format. Effective September 1, 2020: maximum 397 days.	
Subject Distinguished Name		
subject:organisationName (2.5.4.10)		

	Certificate Policies; { 2.23.140.1.1} [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.	
Certificate Transparency (optional)	(1.3.6.1.4.1.11129.2.4.4) This field MAY include two or more Certificate Transparency proofs from approved CT Logs.	
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 or http://crl.quovadisglobal.com/qvsslg2.crl or http://crl.quovadisglobal.com/qvsslg3.crl	
cabfOrganizationIdentifier	cabfOrganizationIdentifier 2.23.140.3.1	Used if subject: organizationIdentifier is used

Purpose of EV SSL

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

- Identify the legal entity that controls a website;
-

- That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the Certificate.

Commitment to Comply with Guidelines

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

Eligible Applicants

QuoVadis issues EV Certificates to Private Organizations, Government Entities, Business Entities and Non-Commercial Entities satisfying the requirements specified below:

i) Private Organization Subjects

- The Private Organization MUST be a legally recognised entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation (e.g., by issuance of a Certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
- The Private Organization MUST have designated with the Incorporating Agency either a Registered Agent or Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;
- The Private Organization MUST NOT be designated on the records of the Incorporating Agency by labels such as
- "inactive," "invalid," "not current," or an equivalent facility;
- The Private Organization MUST have a verifiable physical existence and business presence.
- The Private Organization's Jurisdiction of Incorporation, Registration, Charter, or License and/or its Place of Business MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a Certificate by the laws of Bermuda; and
- The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda.

ii) Government Entity Subjects

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

iii) Business Entity Subjects

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

- The Business Entity MUST be a legally recognised entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, Certificate, or license, and whose existence can be verified with that Registration Agency;
- The Business Entity MUST have a verifiable physical existence and business presence;
- At least one Principal Individual associated with the Business Entity MUST be identified and validated;

- The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;
- Where the Business Entity represents itself under an assumed name, QuoVadis MUST verify the Business Entity's use of the assumed name;
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where QuoVadis is prohibited from doing business or issuing a Certificate under the laws of Bermuda; and
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be listed on any government denial list or prohibited list (such as a trade embargo) under the laws of Bermuda.

iv) Non-Commercial Entity Subjects

- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with QuoVadis that satisfies the requirements of the EV Guidelines or the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: QuoVadis will follow the requirements of the EV Guidelines and maintains a 24/7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or Revoked; and
-

Step 5: All signatures by Certificate Requesters, Certificate Approvers and Contract Signers are verified through follow- up procedures or telephone calls.

Step 6: 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 7: QuoVadis creates the EV Certificate.

Step 8: 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

11.3. QUOVADIS QUALIFIED WEBSITE AUTHENTICATION CERTIFICATE (QCP-w)

QuoVadis Qualified Website Authentication Certificates (QCP-w) (QWAC) are issued under the requirements of ETSI EN 319 411-2 aim to support website authentication based on a Qualified Certificate defined in articles 3 (38) and 45 of the eIDAS Regulation.

QCP-w Certificates issued under these requirements endorse the requirement of EV Certificates whose

Organization Identifier	subject:organisationIdentifier (2.5.4.97)	Refer to: CA/Browser Forum Ballot SC17

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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/qvqwebg1.crt	
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvqwebg1.crl	
cabfOrganizationIdentifier	cabfOrganizationIdentifier 2.23.140.3.1	Used if subject:organizationIdentifier is used
qcStatements		
id-etsi-qcs- QcCompliance	id-etsi-qcs (1 0.4.0.1862.1.1) esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Refer to: ETSI EN 319 412-5
id-etsi-qcs-QcType	id-etsi-qcs-6 (0.4.0.1862.1.6) esi4-qcStatement-6 : Type of certificate Id-etsi-qct-web (0.4.0.1862.1.6.3) id-etsi-qcs-QcType 3 = Certificate for website authentication as defined in Regulation EU No 910/2014	Refer to: ETSI EN 319 412-5

11.4. QUOVADIS QCP-w-psd2

ETSI TS 119 495 defines QWAC profiles and TSP policy requirements under the Payment Services Directive (EU) 2015/2366, which are supplemented by Ballot SC17 of the CA/Browser Forum.

QuoVadis QCP-w-psd2 follow the same profile as QuoVadis QCP-w Certificates with the following variations:

Field	Value	Comments
Subject Distinguished Name		
Organization Identifier	subject:organisationIdentifier (2.5.4.97)	PSD2 Authorisation Number Refer to: ETSI TS 119 495 5.1 CA/Browser Forum Ballot SC17
Extension		

	id-etsi-qcs-QcType 3 = Certificate for website authentication as defined in Regulation EU No 910/2014	
id-etsi-qcs-QcPDS	id-etsi-qcs-5 (0.4.0.1862.1.5) URL= https://www.quovadisglobal.com/repository Language = EN	Refer to: ETSI EN 319 412-5
Etsi-psd2-qcstatement	id-etsi-psd2-qcStatement (0.4.0.19495.2) PSD2QcType ::= SEQUENCE{ rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }	Refer to: ETSI TS 119 495 5.1
id-qcs-pkixQCSyntax-v2	1.3.6.1.55.7.11.2	

Verification Requirements

The verification requirements for a QuoVadis Qualified Website Authentication (QCP-w-PSD) certificate are the same for QCP-w with additional steps to verify PSD2 specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 rolesQuoVadis also confirms the PSD2 role(s) of the Certificate Applicant (RolesOfPSP) in accordance with the rules for validation provided by the NCA, if applicable:

Authorisation Number

The PSD2 Authorisation Number within the certificate takes the following format:

PSD	**NL**	**-**	**DNB**	**-**	**12345Ab**
"PSD" as 3 character identifier for the Registration Scheme					
	2 character ISO 3166 [7] country code representing the NCA country				
		Hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8))			
			2-8 character NCA identifier (A-Z uppercase only, no separator)		
				hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8))	
					PSP identifier (Authorisation Number as specified by the NCA)

NCAs are described by a name "NCAName" and an identifier "NCAId". A list of valid values for "NCAName" and "NCAId" is provided by the EBA (European Banking Authority) and published in ETSI TS 119 495, Annex D.

Note: PSP identifiers MAY contain hyphens, but Registration Schemes, ISO 3166 country codes, and NCA identifiers do not. Therefore if more than one hyphen appears in the final PSP identifier, the leftmost hyphen is a separator and the remaining hyphens are part of the PSP identifier.

PSD2 Roles

The NCA can assign one or more roles (RolesOfPSP) to payment service providers. QuoVadis also confirms the PSD2 role of the Certificate Applicant (RolesOfPSP):

i) account servicing (PSP_AS)

-

11.5. CODESIGNING

Field	Value	Comments
Version	V3	
Serial Number	Unique system generated random number assigned to each certificate, containing at least 64 bits of output.	
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		
Organisation 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.

Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; { 2.23.140.1.4.1 } [1,1] Policy Qualifier Info: Policy Identifier Id=CPS Qualifier:

- A hardware cryptographic module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
- Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Verification Requirements

Before issuing a 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.

Prior to issuing a Code Signing Certificate to an Organisational Applicant, QuoVadis:

i) Verifies the Applicant's possession of the Private Key;

ii) Verifies the Subject's legal identity, including any Doing Business As (DBA) as described in section 3.2.2.2 of the Baseline Requirements,

iii) Verifies the Subject's address, and

iv) 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:

i) the identity of the person performing the verification,

ii) a signed declaration by the verifying person stating that they verified the identity of the Applicant,

iii) a unique identifying number from an identification document of the verifier,

iv) a unique identifying number from an identification document of the Applicant,

v) the date and time of the verification, and

vi) 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 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 Code Signing Certificate.

Step 7: The Certificate is delivered to the Applicant.