Certification Policy/ Certification Practice Statement

OIDs: 1.3.6.1.4.1.8024.0.2

Effective Date:

This document is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited (QuoVadis), a company of DigiCert, Inc. It contains an overview of the practices and procedures that QuoVadis employs for its operation as a Certification Authority (CA). 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 supet/(b)10.9 (j)6st/(2 a)- (t ou)-e ein2loop(c)-5ihe-4.2 (P)0(r)3.3 (s)-4.7 (ion)2.8 (o)-.8 ( )-12 (th)-ebis ( )

QuoVadis PMA	1 December 2006	1.0	Baseline for Root Ceremony
QuoVadis PMA	15 December 2006	1.5	Edits for EV compliance
QuoVadis PMA	28 December 2006	1.6	Formatting and corrections
QuoVadis PMA	12 January 2007	1.7	Corrections to cert policies
QuoVadis PMA	02 October 2007	1.8	v1 of EV Guidelines
QuoVadis PMA	27 May 2008	1.9	V1.1 of EV Guidelines

QuoVadis PMA

4.2.2. Approval Or Rejection Of Certificate Applications 12
4.2.3. Time To Process Certificate Applications 12
4.2.4. Certificate Authority Authorisation (CAA) 12
4.3. Certificate Issuance 13
4.3.1. CA Actions During Certificate Issuance 13
4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate 13
4.4. Certificate Acceptance 13
4.4.1. Conduct Constituting Certificate Acceptance 13
4.4.2. Publication Of The Certificate By The CA 13
4.4.3. Notification Of Certificate Issuance By The CA To Other Entities 13
4.5. Key Pair And Certificate Usage 13
4.5.1. Subscriber Private Key And Certificate Usage 13
4.5.2. Relying Party Public Key And Certificate Usage 13
4.6. Certificate Renewal 14
4.6.1. Circumstance For Certificate Renewal 14
4.6.2. Who May Request Renewal 14
4.6.3. Processing Certificate Renewal Requests 14
4.6.4. Notification of New Certificate Issuance To Subscriber 14
4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate 14
4.6.6. Publication of the Renewal Certificate By The CA 14
4.6.7. Notification Of Certificate Issuance By The CA To Other Entities 15
4.7. Certificate Re-Key 15
4.7.1. Circumstance for Certificate Re-Key 15
4.7.2. Who May Request Re-Key 15
4.7.3. Processing Certificate Re-Key Request 15
4.7.4. Notification of Certificate Re-Key To Subscriber 15
4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate 15
4.7.6. Publication of The Re-Key Certificate By The CA 15
4.7.7. Notification of Certificate Re-Key By The CA To Other Entities 15
4.8. Certificate Modification 15
4.8.1. Circumstances For Certificate Modification 15
4.8.2. Who May Request Certificate Modification 16
4.8.3. Processing Certificate Modification Requests 16
4.8.4. Notification Of Certificate Modification To Subscriber 16
4.8.5. Conduct Constituting Acceptance Of A Modified Certificate 16
4.8.6. Publication Of The Modified Certificate By The CA 16
4.8.7. Notification Of Certificate Modification By The CA To Other Entities 16
4.9. Certificate Revocation And Suspension 16
4.9.1. Circumstances For Revocation 16
4.9.2. Who Can Request Revocation 18
4.9.3. Procedure For Revocation Request 18
4.9.4. Revocation Request Grace Period 19
4.9.5. Time Within Which The CA Must Process The Revocation Request 19
4.9.6. Revocation Checking Requirement For Relying Parties 19
4.9.7. CRL Issuance Frequency 19
4.9.8. Maximum Latency...e5 ..... (y)-7.7 ɑssuance Frt 19

4.10.2. Service Availability 20
4.10.1. Optional Features 20
4.11. End Of Subscription 20
4.12. Key Escrow And Recovery 20
4.12.1. Key Archival Escrow And Recovery Policy And Practices 20
4.12.2. Session Key Encapsulation And Recovery Policy And Practices 20
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 21
5.1. Physical Controls 21
5.1.1. Site Location and Construction 21
5.1.2. Physical Access 21
5.1.3. Power And Air-Conditioning 21
5.1.4. Water Exposures 21
5.1.5. Fire Prevention And Protection 21
5.1.6. Media Storage 22
5.1.7. Waste Disposal 22
5.1.8. Off-Site Backup 22
5.2. Procedural Controls 22
5.2.1. Trusted Roles 22
5.2.2. Number Of Persons Required Per Task 23
5.2.3. Identification And Authentication For Each Role 23
5.2.4. Roles Requiring Separation Of Duties 23
5.3. Personnel Controls 23
5.3.1. Qualifications, Experience, And Clearance Requirements 23
5.3.2. Background Check Procedures 23
5.3.3. Training Requirements 24
5.3.4. Retraining Frequency And Requirements 24
5.3.5. Job Rotation Frequency And Sequence 24
5.3.6. Sanctions For Unauthorised Actions 24
5.3.7. Independent Contractor Requirements 24
5.3.8. Documentation Supplied To Personnel 24
5.4. Audit Logging Procedures 25
5.4.1. Types Of Events Recorded 25
5.4.2. Frequency Of Processing Log 25
5.4.3. Retention Period For Audit Log 25
5.4.4. Protection Of Audit Log 25
5.4.5. Audit Log Backup Procedures 25
5.4.6. Audit Collection System 26
5.4.7. Notification To Event-Causing Subject 26
5.4.8. Vulnerability Assessment 26
5.5. Records Archival 26
5.5.1. Types Of Records Archived 26
5.5.2. Retention Period For Archive 26
5.5.3. Protection Of Archive 26
5.5.4. Archive Backup Procedures 27
5.5.5. Requirements For Time-Stamping Of Records 27
5.5.6. Archive Collection System 27
5.5.7. Procedu
7oce4-7.718(r)6.7 8rs (n)4 (r)6a3 (e)-3in seee4-716 (7ocif4 (m7-2.3 0(f)4.7 (1(e)0.6 (e)06 (och3 (u)7iv3

8.3. Assessor's Relationship To Assessed Entity 37
8.4. Topics Covered By Assessment 37
8.5. Actions Taken As A Result Of Deficiency 37
8.6. Publication Of Audit Results 37
8.7. Self Audits 37
9. OTHER BUSINESS AND LEGAL MATTERS 38
9.1. Fees 38
9.1.1. Certificate Issuance Or Renewal Fees 38
9.1.2. Certificate Access Fees 38
9.1.3. Revocation Or Status Information Access Fees 38
9.1.4. Fees For Other Services 38
9.1.5. Refund Policy 38
9.2. Financial Responsibilities 38
9.2.1. Insurance Coverage 38
9.2.2. Other Assets 38
9.2.3. Insurance Or Warranty Coverage For End-Entities 38
9.2.[illegible]
9.3.1. Scope Of Confidential Information 39
9.3.2. Information Not Within The Scope.7 (o)-(7 T.....t.....t.....i.4 (h)7.3 (e)-3.3 (S)4.7 (c)3 (o)13 (p)-2

9.16. Miscellaneous Provisions....47
9.16.1. Entire Agreement....47
9.16.2. Assignment....47
9.16.3. Severability....47
9.16.4. Enforcement (Waiver Of Rights)

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 Orgnisation 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 trust services for electronic transactions in the internal market (the "eIDAS Regulation")QuoVadis is a Qualified Trust Service Provider (TSP) listed on the Trusted List for the Netherlands (https://webgate.ec.europa.eu/tl-browser/#/trustmark/NL/NTRNL-30237459.

iv) Code Signing Certificates are Certificates issued in compliance with the Code Signing Minimum Requirements, including identification of the Certificate subject by a verified organization name and Certificate revocation for any misrepresentation or publication of malicious code.

QuoVadis Certificates comply with Internet standards (x509 v.3) as set out in RFC 5280. This CP/CPS follows the IETF PKIX RFC 3647 framework with 9 sections that cover practices and procedures for identifying Certificate applicants; issuing and revoking Certificates; and the security controls related to managing the physical, personnel, technical, and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some sections will have the statement "Not applicable" or "No Stipulation."

- 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).

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 CMS is a secure web application that facilitates RAs' activities as well as the ongoing man

: 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.

: 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.

CA	Certificate Authority or Certification Authority
CAA	Certificate Authority Authorisation
CMS	Certificate Management System
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

number used must be the number listed by the Domain Name Registrar. Performed in

Certificate Requests must be in a

ICANN root QuoVadis documents potential issuances that were prevented by a CAA record, and may not

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.

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.

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

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

QuoVadis B Pu59.28 Tm(5l)-67j/TT2 1 oe6 Ee Mi901--Ticate B REV Tw 1O(w)1C y wTertif[( )3 16Tic

iii) QuoVadis confirms any circumstance indicating that use of a FQDN, IP address, or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the

QuoVadis always revokes a Certificate if the binding between the subject and the subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

QuoVadis will revoke a Issuing CA Certificate within seven (7) days after confirming one or more of the following occurred:

i) The Issuing CA requests revocation in writing;

ii) The Issuing CA notifies QuoVadis that the original Certificate Request was not authorised and does not retroactively grant authorisation;

iii) QuoVadis obtains evidence that the Issuing CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;

iv) QuoVadis obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;

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 suppliers or Relying Parties.

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 Suppliers, and other third parties (such as a National Competent Authority that issued the Authorisation Number in a PSD2 Certificate) with clear instructions on how they can report suspected Private Key compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates on the following website: https://www.quovadisglobal.com/certificate-revocation.

QuoVadis processes a revocation request as follows:

i) QuoVadis logs the identity of entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. QuoVadis may also include its own reasons

iv) For requests from third parties, QuoVadis personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

- the nature of the alleged problem;
- the number of reports received about a particular Certificate or website;
- the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
- relevant legislation.

v) If QuoVadis determines that revocation is appropriate, QuoVadis personnel revoke the Certificate and update the CRLIf QuoVadis deems appropriate, QuoVadis may forward the revocation reports to law enforcement.

QuoVadis maintains a continuous 24x7 ability to internally respond to high priority revocation requests

accordance with the Baseline Requirements. The CRLReason for non-issued Certificates is “certificateHold” (value 6).

Not applicable.

QuoVadis uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private KeyQuoVadis will select the CRLReason code “keyCompromise” (value 1) upon discovery of such reason or as required by an applicable CP/CPS. Should a CA Private Key become compromised, QuoVadis shall revoke all Certificates issued by that CA.

The QuoVadis PKI does not support suspension of Certificates.

The QuoVadis PKI does not support suspension of Certificates.

The QuoVadis PKI does not support suspension of Certificates.

The QuoVadis PKI does not support suspension of Certificates.

4.10. CERTIFICATE STATUS SERVICES

Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked Certificate. The exception to this is revoked Code Signing Certificates, which remain on the CRL for at least 10 years following the expiry date.

Certificate status services are available 24x7.

No

5.2.1.5. RA Administrators

RA Administrators manage the RA CMS, including the assignment of Issuing CAs and Certificate Profiles to customer accounts.

5.2.1.6. Security Officers

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

to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. AUDIT LOGGING PROCEDURES

QuoVadis maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

iii) If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;

iv) If the compromise involves a Private Key used to sign time-stamp tokens, provide a description of the compromise to Subscribers and Relying Parties;

v) Make information available that can be used to identify which Certificates and time-stamp tokens are affected, unless doing so would breach the privacy of a QuoVadis user or the security of QuoVadis' services;

vi) Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;

vii) Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;

viii) Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and

ix) Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

QuoVadis may generate a new Key Pair and sign a new Certificate. If a disaster physically damages QuoVadis' equipment and destroys all copies of QuoVadis' Private Keys then QuoVadis will provide notice to affected parties at the earliest feasible time.

To maintain the integrity of its services, QuoVadis implements data backup and recovery procedures as part

transported between cryptographic modules, QuoVadis encrypts the Private Key and protects the keys used

Publicly Trusted Issuing CAs	10 - 15 years
Business SSL Certificates	825 days (398 days after September 1, 2020)
EV SSL Certificates	2 years (398 days after September 1, 2020)
Qualified Web Authentication Certificates (QCP-w)	2 years (398 days after September 1, 2020)

Participants shall cease all use of their Key Pairs after their usage periods have expired. Relying Parties may still validate signatures generated with these keys after expiration of the Certificate.

QuoVadis may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. QuoVadis does not issue Subscriber Certificates with an expiration date that exceeds the Issuing CA's term or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4. ACTIVATION DATA

QuoVadis activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer, meeting the requirements of FIPS 140-2 Level 3 and/or Common Criteria EAL 4. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in 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.

6.7. 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, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to

ii) For each iPAddress range in permittedSubtrees, QuoVadis confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

iii) For each DirectoryName in permittedSubtrees QuoVadis confirms the Applicant's and/or Subsidiary's Organisational name(s) and location(s) such that end entity Certificates issued from the Issuing CA will comply with section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements.

If the Issuing CA is not allowed to issue certificates with an iPAddress, then the Issuing CA Certificate specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Issuing CA Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Issuing CA Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Issuing CA Certificate includes at least one iPAddress in permittedSubtrees.

If the Issuing CA is not allowed to issue certificates with dNSNames, then the Issuing CA Certificate includes a zero-length dNSName in excludedSubtrees. Otherwise, the Issuing CA Certificate includes at least one dNSName in permittedSubtrees.

7.1.6.

An object identifier (OID) is a number unique that identifies an object or policy. The Certificate Policy OIDs that incorporate this CP/CPS into different Certificate P.8 (t Ca -0 0 1e-N D)-1.6 (s)--(tif)00.8 ( ).8 (i22)]TJ-33.9,(in)2.--2 (l)-3 (i

QuoVadis CRLs have the following extensions:

CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Reason for revocation

7.3. ONLINE CERTIFICATE STATUS PROTOCOL PROFILE

OCSP is enabled for all Certificates within the QuoVadis PKI.

OCSP Version 1, as defined by RFC 2560, is supported within the QuoVadis PKI.

Not applicable.

7.4. CERTIFICATE TRANSPARENCY

QuoVadis TLS/SSL Certificates MAY include Signed Certificate Timestamps (SCT) from independent CT Logs. Information on Certificate Transparency may be found in IETF RFC 6962.

8.1. FREQUENCY, CIRCUMSTANCE AND STANDARDS OF ASSESSMENT

The practices s(P)1 (Lr)10.4 (ac-2 (A)/v6H6f1d)1.2 (-12.5 (ou)-92 (in))1.2 (T)8. (A)/.5 2 (og (ti)(,)2.1 (Pc-2 (A/) (i),)2.1 (Pc-2

9.1. FEES

QuoVadis charges fees for verification, certificate issuance and renewal. QuoVadis may change its fees at any time in accordance with the applicable customer agreement

QuoVadis may charge a reasonable fee for access to its certificate databases.

QuoVadis does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. QuoVadis may charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. QuoVadis does not permit access to revocation information, Certificate status information, or time stamping in their Repositories by third parties that provide products or services that utilize such Certificate status information without QuoVadis' prior express written consent.

QuoVadis does not charge a fee for access to this CP/CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

QuoVadis may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. FINANCIAL

registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly

iv) Promptly (a) request revocation of a Certificate, cease using it and its associated Private Key, and notify QuoVadis if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (b) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

v) Ensure that individuals using Certificates on behalf of an organisation have received security training appropriate to the Certificate;

vi) Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, including only installing TLS/SSL Server Certificates on servers accessible at the Domain listed in the Certificate a8 (te)tTi8h3.6 (s)-4.87(d)-2.9(i)-2.3(n)-2.5(s)-0.0(0)0.7(0)6

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.

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.

9.9. INDEMNITIES

9.12. AMENDMENTS

9.16. MISCELLANEOUS PROVISIONS

QuoVadis contractually obligates each RA to comply with this CP/

Version	V3
Serial Number	Unique number 0509
Issuer Signature Algorithm	sha-

Version	V3
Serial Number	Unique number 445734245b81899b35f2ceb82b3b5ba726f07528
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 G3 O =QuoVadis Limited C = BM
Validity Period	30 years expressed in UTC format NotBefore: 01/12/2012 18:59:32 NotAfter: 01/12/2042 18:59:32
Subject Distinguished Name	CN = QuoVadis Root CA 2 G3 O =QuoVadis Limited C = BM
Subject Public Key Information	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 4096-bit
Issuer's Signature	sha256RSA {1.2.840.113549.1.1.11 }
Subject Key Identifier	c=no; ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=None
Key Id Hash(sha1):	67 ec 9f 90 2d cd 64 ae fe 7e bc cd f8 8c 51 28 f1 93 2c 12
Cert Hash(sha1):	09 3c 61 f3 8b 8b dc 7d 55 df 75 38 02 05 00 e1 25 f5 c8 36

11.1. BUSINESS SSL

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.quovadisgl1 (L)-4.ff

: 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)

ceName (1.3.6.1.4.1.311.60.2.1.2)	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.	ceName (1.3.6.1.4.1.311.60.2.1.2)
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.	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)
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.	

registration. 74.8 (o)-6.9 (r)0.9 (a)-4.6 (t)-6.6 (i)-7.0 (o)-5.6 (n)-E9.3 t(E)-442 (n)2.8 (ti)-12.2 (tie)-7 (s)-4

- Contract Signer: MUST be either the Applicant, employed by the Applicant, or an authorised agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
- Confirming Person: Must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) able to sign the QV Authority Letter on behalf of the Applicant.

Each Applicant must enter into a Subscriber Agreement with QuoVadis which specifically names both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf, and contains provisions imposing on the Applicant the following obligations and warranties:

- Accurac alrovisionsigartAp7 (n)2.8io6 (th)-3.3 (if)0oarrapp ( )TjEMC /d:nt th-7 (c)7.77 (c) (,u (p)0.7 (p)-1h)-3.2ob

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 purpose is specified in clause 5.5 of ETSI EN 319 411-1 [2]. QWACs issued under this policy provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website as specified in the eIDAS Regulation.

The QuoVadis QWAC is designed to comply with:

- CA/Browser Forum EV Guidelines;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Requirements for Trust Service Providers issuing EU Qualified Certificates;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate profile for web site certificates; and
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); QCStatements

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		

Organisation Unit	subject:organisationUnit (2.5.6.5)	No longer permitted in EV SSL
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard Certificates are not allowed for EV Certificates.
City or Town of Incorporation	subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows.
State/ Province of Incorporation	subject: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 Registra or4ntrr5.1 (s)-7e o rpa6.8 ( )

	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	Optional Refer to: CA/Browser Forum Ballot SC17

id-etsi-qcs- QcCompliance id-etsi-

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:

Organization Identifier	subject:organisationIdentifier (2.5.4.97)	PSD2 Authorisation Number Refer to: ETSI TS 119 495 5.1 CA/Browser Forum Ballot SC17

Certificate Policies

c=no;

[1] Certificate Policy:
Policy Identifier=0.4.0.194112.1.4

[2] Certificate Policy:
Policy Identifier=
1.3.6.1.4.1.8024.0.2.100.1.2

[3] Certificate Policy:
Policy Identifier=
1.3.6.1.4.1.8024.1.450

[3,1] Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.quovadisgloba
l.(:)-2 (/7.88 558.48 HS(=)-11.0 Tc (:)]Tm)e 541Uw

	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	

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 Authori

- OID: id-psd2-role-psp-