digicert + QuoVadis

QuoVadis Root CA2 Certification Policy/ Certification Practice Statement

OID:	1.3.6.1.4.1.8024.0.2
Effective Date:	June 7, 2019
Version:	2.6

Important Note About this Document

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

Contact Information:

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

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

Website: http://www.quovadisglobal.com

e-mail: compliance@quovadisglobal.com

Version Control

Author	Date	Version	Comment
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	Revisions for v1 of EV Guidelines
QuoVadis PMA	27 May 2008	1.9	Updated to reflect V1.1 of EV Guidelines
QuoVadis PMA	22 April 2010	1.10	Update for EV Guidelines Errata and revised Certificate Holder Agreement
QuoVadis PMA	1 March 2012	1.11	Update of revocation reasons as well as changes to EV policies and prohibition of MITM
QuoVadis PMA	12 July 2012	1.12	Update for Baseline Requirements
QuoVadis PMA	31 January 2013	1.13	Updates for SHA256 Roots
QuoVadis PMA	11 March 2014	1.14	Update for SHA256 Code Signing CA and update to physical controls section
QuoVadis PMA	27 May 2014	1.15	Updates to links to QuoVadis Website and archive periods
QuoVadis PMA	5 August 2014	1.16	Addition of ICA certificate profiles
QuoVadis PMA	26 January 2015	1.17	Update for Certificate Transparency
QuoVadis PMA	15 April 2015	1.18	Updates to Certification Authority Authorisation (CAA) policy
QuoVadis PMA	24 February 2017	1.19	Updates for Code Signing Minimum Requirements
QuoVadis PMA	8 May 2017	2.0	Introduces eIDAS Qualified Website Authentication Certificates.
QuoVadis PMA	3 July 2017	2.1	Updates to domain validation requirements
QuoVadis PMA	6 September 2017	2.2	Updates for Certificate Authority Authorisation (CAA). Updates for submission of complaints.

QuoVadis PMA	31 January 2018	2.3	Updates for the Baseline Requirements and Mozilla Root Store Policy
QuoVadis PMA	30 July 2018	2.4	Updates for domain vetting (ballot 218)
QuoVadis PMA	7 December 2018	2.5	Updates for the Baseline Requirements and addition of ICA profiles. More explicit reference to the BR Domain Vetting methods.
QuoVadis PMA	7 June 2019	2.6	Updates for Baseline Requirements domain and IP address validation methods. Changes to CRL update.

Table of Contents

1 Introduction 11
1.1 Overview 11
1.2 Document Name And Identification 12
1.3 PKI Participants 12
1.3.1 1.3.1. Certification Authority 12
1.3.2 Registration Authorities 13
1.3.3 Certificate Holders 14
1.3.4 Relying Parties 14
1.4 Certificate Usage 15
1.4.1 Appropriate Certificate Uses 15
1.4.2 Prohibited Certificate Usage 15
1.5 Policy Administration 15
1.5.1 Organisation Administering the CP/CPS 15
1.5.2 CP/CPS Approval Procedures 15
1.6 Definitions and Acronyms 16
2 Publication and Repository Responsibilities 19
2.1 Repositories 19
2.2 Publication of Certificate Information 19
2.3 Time or Frequency of Publication 20
2.4 Access Controls on Repositories 20
3 Identification and Authentication 21
3.1 Naming 21
3.1.1 Types Of Names 21
3.1.2 Need For Names To Be Meaningful 21
3.1.3 Pseudonymous Certificate Holders 21
3.1.4 Rules For Interpreting Various Name Forms 21
3.1.5 Uniqueness Of Names 22
3.1.6 Recognition, Authentication, And Role Of Trademarks 22
3.2 Initial Identity Validation 22
3.2.1 Method To Prove Possession Of Private Key 22
3.2.2 Authentication Of Organisation Identity 22
3.2.3 Authentication Of Individual Identity 25
3.2.4 Non-Verified Certificate Holder Information 25
3.2.5 Validation Of Authority 25
3.3 Identification And Authentication For Re-Key Requests 25
3.3.1 Identification And Authentication For Routine Re-Key 25
3.3.2 Identification and Authentication For Re-Key After Revocation 26
3.4 Identification and Authentication For Revocation Requests 26

4 Certificate Life-Cycle Operation Requirements 27
4.1 Certificate Application 27
4.2 Certificate Application Processing 27
4.2.1 Performing Identification And Authentication Functions 27
4.2.2 Approval Or Rejection Of Certificate Applications 27
4.2.3 Time To Process Certificate Applications 27
4.2.4 Certificate Authority Authorisation (CAA) 28
4.3 Certificate Issuance 28
4.3.1 CA Actions During Certificate Issuance 28
4.3.2 Notification To Certificate Holder By The CA Of Issuance Of Certificate 29
4.4 Certificate Acceptance 29
4.4.1 Conduct Constituting Certificate Acceptance 29
4.4.2 Publication Of The Certificate By The CA 29
4.5 Key Pair And Certificate Usage 29
4.5.1 Certificate Holder Private Key And Certificate Usage 29
4.5.2 Relying Party Public Key And Certificate Usage 29
4.6 Certificate Renewal 30
4.7 Certificate Re-Key 30
4.8 Certificate Modification 30
4.9 Certificate Revocation And Suspension 31
4.9.1 Circumstances For Revocation 31
4.9.2 Who Can Request Revocation 32
4.9.3 Procedure For Revocation Request 33
4.9.4 Revocation Request Grace Period 33
4.9.5 Time Within Which The CA Must Process The Revocation Request 33
4.9.6 Revocation Checking Requirement For Relying Parties 34
4.9.7 CRL Issuance Frequency 34
4.9.8 Maximum Latency For CRL 34
4.9.9 On-Line Revocation/Status Checking Availability 34
4.9.10 On-Line Revocation Checking Requirement 34
4.9.11 Other Forms Of Revocation Advertisements Available 34
4.9.12 Special Requirements for Key Compromise 34
4.9.13 Circumstances For Suspension 35
4.9.14 Who Can Request Suspension 35
4.9.15 Procedure For Suspension Request 35
4.9.16 Limits On Suspension Period 35
4.10 Certificate Status Services 35
4.10.1 Operational Characteristics 35
4.10.2 Service Availability 35
4.11 End Of Subscription 35
4.12 Key Escrow And Recovery 35

5 Facility, Management, and Operational Controls 36
5.1 Physical Controls 36
5.1.1 Site Location and Construction 36
5.1.2 Physical Access 36
5.1.3 Power And Air-Conditioning 37
5.1.4 Water Exposures 37
5.1.5 Fire Prevention And Protection 37
5.1.6 Media Storage 37
5.1.7 Waste Disposal 37
5.1.8 Off-Site Backup 37
5.2 Procedural Controls 37
5.2.1 Trusted Roles 38
5.2.2 Number Of Persons Required Per Task 38
5.2.3 Identification And Authentication For Each Role 38
5.2.4 Roles Requiring Separation Of Duties 38
5.3 Personnel Controls 39
5.3.1 Qualifications, Experience, And Clearance Requirements 39
5.3.2 Background Check Procedures 39
5.3.3 Training Requirements 39
5.3.4 Retraining Frequency And Requirements 40
5.3.5 Job Rotation Frequency And Sequence 40
5.3.6 Sanctions For Unauthorised Actions 40
5.3.7 Independent Contractor Requirements 40
5.3.8 Documentation Supplied To Personnel 40
5.4 Audit Logging Procedures 40
5.4.1 Types Of Events Recorded 40
5.4.2 Frequency Of Processing Log 41
5.4.3 Retention Period For Audit Log 41
5.4.4 Protection Of Audit Log 41
5.4.5 Audit Log Backup Procedures 41
5.4.6 Audit Collection System 41
5.4.7 Notification To Event-Causing Subject 42
5.4.8 Vulnerability Assessment 42
5.5 Records Archival 42
5.5.1 Types Of Records Archived 42
5.5.2 Retention Period For Archive 42
5.5.3 Protection Of Archive 42
5.5.4 Archive Backup Procedures 43
5.5.5 Requirements For Time-Stamping Of Records 43
5.5.6 Archive Collection System 43
5.5.7 Procedures To Obtain And Verify Archive Information 43
5.6 Key Changeover 43
5.7 Compromise And Disaster Recovery 43

5.7.1 QuoVadis Business Continuity Plan 44
5.8 CA And/Or RA Termination 44
6 Technical Security Controls 45
6.1 Key Pair Generation And Installation 45
6.1.1 Key Pair Generation 45
6.1.2 Private Key Delivery To Certificate Holder 45
6.1.3 Public Key Delivery To Certificate Issuer 45
6.1.4 Certification Authority Public Key To Relying Parties 45
6.1.5 Key Sizes 45
6.1.6 Public Key Parameters Generation And Quality Checking 46
6.1.7 Key Usage Purposes (As Per X.509 V3 Key Usage Field) 46
6.2 Private Key Protection And Cryptographic Module Engineering Controls 46
6.2.1 Cryptographic Module Standards And Controls 46
6.2.2 Private Key (N Out Of M) Multi-Person Control 46
6.2.3 Private Key Escrow 47
6.2.4 Private Key Backup 47
6.2.5 Private Key Archive 47
6.2.6 Private Key Transfer Into Or From A Cryptographic Module 47
6.2.7 Private Key Storage On Cryptographic Module 47
6.2.8 Method Of Activating Private Key 47
6.2.9 Method Of Deactivating Private Key 47
6.2.10 Method Of Destroying Private Key 48
6.2.11 Cryptographic Module Rating 48
6.3 Other Aspects Of Key Pair Management 48
6.3.1 Public Key Archival 48
6.3.2 Certificate Operational Periods And Key Pair Usage Periods 48
6.4 Activation Data 48
6.4.1 Activation Data Generation And Installation 48
6.4.2 Activation Data Protection 49
6.4.3 Other Aspects Of Activation Data 49
6.5 Computer Security Controls 49
6.5.1 Specific Computer Security Technical Requirements 49
6.5.2 Computer Security Rating 49
6.6 Life Cycle Technical Controls 50
6.6.1 System Development Controls 50
6.6.2 Security Management Controls 50
6.6.3 Life Cycle Security Controls 50
6.7 Network Security Controls 50
6.8 Time-Stamping 51
7 Certificate, CRL, and OCSP Profiles 52
7.1 Certificate Profile 52

7.1.1 Version Numbers 52
7.1.2 Certificate Extensions 52
7.1.3 Algorithm Object Identifiers 52
7.1.4 Name Forms 52
7.1.5 Name Constraints 52
7.1.6 Certificate Policy Object Identifier 52
7.1.7 Usage Of Policy Constraints Extension 53
7.1.8 Policy Qualifiers Syntax And Semantics 53
7.1.9 Processing Semantics For The Critical Certificate Policies Extension 53
7.2 CRL Profile 53
7.2.1 Version Number 53
7.2.2 CRL And CRL Entry Extensions 53
7.3 Online Certificate Status Protocol Profile 54
7.3.1 Online Certificate Status Protocol Version Numbers 54
7.3.2 Online Certificate Status Protocol Extensions 54
7.4 Certificate Transparency 54
8 Compliance Audit and Other Assessments 55
8.1 Frequency, Circumstance And Standards Of Assessment 55
8.2 Identity And Qualifications Of Assessor 55
8.3 Assessor's Relationship To Assessed Entity 55
8.4 Topics Covered By Assessment 55
8.5 Actions Taken As A Result Of Deficiency 56
8.6 Publication Of Audit Results 56
8.7 Self Audits 56
9 Other Business and Legal Matters 57
9.1 Fees 57
9.1.1 Certificate Issuance Or Renewal Fees 57
9.1.2 Certificate Access Fees 57
9.1.3 Revocation Or Status Information Access Fees 57
9.1.4 Fees For Other Services 57
9.1.5 Refund Policy 57
9.2 Financial Responsibilities 57
9.2.1 Financial Records 57
9.2.2 No Partnership or Agency 58
9.2.3 Insurance Cover 58
9.2.4 Other Assets 58
9.2.5 Insurance Or Warranty Coverage For End-Entities 58
9.3 Confidentiality Of Business Information 58
9.3.1 Scope Of Confidential Information 58
9.3.2 Information Not Within The Scope Of Confidential Information 59
9.4 Responsibility To Protect Private Information 59

9.4.1 Privacy Plan 59
9.4.2 Information Treated As Private 59
9.4.3 Information Deemed Not Private 60
9.4.4 Responsibility To Protect Private Information 60
9.4.5 Notice And Consent To Use Private Information 60
9.4.6 Disclosure Pursuant To Judicial Or Administrative Process 60
9.5 Intellectual Property Rights 60
9.6 Representations And Warranties 61
9.6.1 Certification Authority Representations 61
9.6.2 Third Party LRA Representations and Warranties 61
9.6.3 Certificate Holder Representations And Warranties 62
9.6.4 Relying Parties Representations And Warranties 63
9.6.5 Representations And Warranties Of Other Participants 64
9.7 Disclaimers Of Warranties 64
9.8 QuoVadis Liability 65
9.8.1 Limitations of Liability 65
9.8.2 Exclusions of Liability 66
9.8.3 Certificate Loss Limits 67
9.9 Indemnities 67
9.10 Term And Termination 68
9.10.1 Term 68
9.10.2 Termination 68
9.10.3 Effect Of Termination And Survival 68
9.11 Individual Notices And Communications With Participants 68
9.12 Amendments 69
9.12.1 Procedure For Amendment 69
9.12.2 Notification Mechanism And Period 69
9.12.3 Circumstances Under Which OID Must Be Changed 69
9.13 Dispute Resolution Provisions 69
9.14 Governing Law 70
9.15 Compliance With Applicable Law 70
9.16 Miscellaneous Provisions 70
9.16.1 Entire Agreement 70
9.16.2 Assignment 70
9.16.3 Severability 70
9.16.4 Enforcement (Waiver Of Rights) 70
9.16.5 Force Majeure 71
9.17 Other Provisions 71
10 APPENDIX A – CA Profiles 72
11 APPENDIX B 85
11.1 Business SSL 85

11.2 Extended Validation SSL 89
11.3 QuoVadis Qualified Website Authentication (QCP-w)..... 100
11.4 Code Signing 105

1 Introduction

1.1 Overview

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

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

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that QuoVadis Root CA2 uses in the generation, issue, use, and management of Certificates and serves to notify Certificate Holders and Relying Parties of their roles and responsibilities concerning Certificates. The term “QuoVadis Root CA2” applies to all generations of this Root, including the SHA1 and SHA256 versions.

QuoVadis ensures the integrity of its Public Key Infrastructure (PKI) operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between QuoVadis and any Participant in the QuoVadis PKI. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation.

QuoVadis issues three forms of Certificates according to the terms of this CP/CPS:

I. Business SSL Certificates are Certificates for which limited authentication and authorization checks are performed on the Certificate Holder and the individuals acting for the Certificate Holder.
II. Extended Validation SSL Certificates are Certificates 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 Certificate Holder by enforcing uniform and detailed validation procedures across all EV-issuing CAs.
III. 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 (which supersedes RFC 3280). This CP/CPS follows the IETF PKIX RFC 3647

framework with 9 sections that cover practices and procedures for identifying Certificate applicants; issuing and revoking Certificates; and the security controls related to managing the physical, personnel, technical, and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some sections will have the statement "Not applicable" or "No Stipulation."

Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS Regulation”) came into force on 1 July 2016. QuoVadis is listed on the Trusted List for the Netherlands (https://webgate.ec.europa.eu/tl-browser/#/trustmark/NL/NTRNL-30237459) for Qualified certificates for website authentication in accordance with the eIDAS Regulation.

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 is 1.3.6.1.4.1.8024.0.2.

The provisions of this CP/CPS, as amended on at least an annual basis, are incorporated by reference into all QuoVadis Certificates that are issued on or after the effective date of publication of this CP/CPS. QuoVadis shall make amendments to this CP/CPS in accordance with Section 9.10.

1.3 PKI Participants

Participants (Participants) within the QuoVadis PKI include:

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

1.3.1 1.3.1. Certification Authority

The following OIDs are pertinent to this CP/CPS:

QuoVadis Root CA2/ QuoVadis Root CA 2 G3	1.3.6.1.4.1.8024.0.2
QuoVadis Global SSL ICA (all generations)	1.3.6.1.4.1.8024.0.2.100.1
QuoVadis Business SSL	1.3.6.1.4.1.8024.0.2.100.1.1
QuoVadis Extended Validation SSL	1.3.6.1.4.1.8024.0.2.100.1.2
QuoVadis Code Signing	1.3.6.1.4.1.8024.0.2.200.1.1

The inclusion of the QuoVadis Business SSL OID (1.3.6.1.4.1.8024.0.2.100.1.1) in the certificatePolicies extension of an end entity certificate asserts adherence to and compliance with the Baseline Requirements.

The inclusion of the QuoVadis Extended Validation SSL OID (1.3.6.1.4.1.8024.0.2.100.1.2) in the certificatePolicies extension of an end entity certificate asserts adherence to and compliance with the EV Guidelines.

The inclusion of the QuoVadis Code Signing OID (1.3.6.1.4.1.8024.0.2.200.1.1) in the certificatePolicies extension of an end entity certificate asserts adherence to and compliance with the Code Signing Minimum Requirements.

QuoVadis Root CA2 and its underlying Issuing CAs issue Certificates to Certificate Holders in accordance with this CP/CPS. In its role as a CA, QuoVadis performs functions associated with public key operations that include receiving requests; issuing, revoking and renewing a Certificate; and the maintenance, issuance, and publication of CRLs for users within the QuoVadis PKI. In its capacity as a CA, QuoVadis will:

- Conform its operations to this CP/CPS (or other relevant business practices);
- Issue and publish Certificates in a timely manner;
- Perform verification of Certificate Holder information in accordance with this CP/CPS;
- Revoke Certificates upon receipt of a valid request from an authorised person or on its own initiative when circumstances warrant; and
- Notify Certificate Holders 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. QuoVadis will not issue a subordinate Issuing CA Certificate to be used for these purposes.

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 Certificate Holder 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.

QuoVadis' Trust/Link Enterprise 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 Certificate Holders

In the context of this CP/CPS, the Certificate Holder is the Individual responsible for requesting, installing and maintaining the trusted system for which a TLS/SSL Certificate has been issued. The Certificate Holder is referred to as a Subscriber in the Trust/Link system. (QuoVadis also refers to Registrants for End User Certificates as Certificate Holders). Prior to verification of identity and issuance of a Certificate, a Certificate Holder is an Applicant for QuoVadis services.

Before accepting and using a Certificate, a Certificate Holder must: (i) generate its own key pair; (ii) submit an application for a QuoVadis Certificate; and (iii) accept and agree to the terms and conditions of the applicable QuoVadis Certificate Holder Agreement. The Certificate Holder is solely responsible for the generation of the key pair to which its QuoVadis Certificate relates and for the protection of the Private Key underlying the QuoVadis Certificate. A Certificate Holder shall immediately notify QuoVadis if any information contained in a QuoVadis Certificate changes or becomes false or misleading, or in the event that its private key has been compromised or the Certificate Holder suspects that it has been compromised. A Certificate Holder must immediately stop using a Certificate and delete it from the Certificate Holder's server upon revocation or expiration.

1.3.4 Relying Parties

Relying Parties are Individuals or Organisations who reasonably rely on QuoVadis Certificates in accordance with the terms and conditions of this CP/CPS and all applicable laws and regulations.

Before relying on or using a QuoVadis Certificate, Relying Parties are advised to: (i) read this CP/CPS in its entirety; (ii) visit the QuoVadis Repository to determine whether the Certificate has expired or been revoked and to find out more information concerning the Certificate; and (iii) make their own judgment as to whether and to what degree to rely upon a Certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate.

1.4.2 Prohibited Certificate Usage

QuoVadis Certificates may not be used and no participation is permitted in the QuoVadis PKI (i) in circumstances that breach, contravene, or infringe the rights of others; or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order; or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

No reliance may be placed on Certificates and Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use; (ii) in breach of this CP/CPS or the relevant Certificate Holder Agreement; (iii) in any circumstances where the use of Certificates could lead to death, injury, or damage to property; or (iv) as otherwise may be prohibited by the terms of issue.

1.5 Policy Administration

1.5.1 Organisation Administering the CP/CPS

This CP/CPS and related agreements and security policy documents referenced within this document are administered by the QuoVadis Policy Management Authority (PMA).

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

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

e-mail: compliance@quovadisglobal.com

1.5.2 CP/CPS Approval Procedures

Approval of this CP/CPS and any amendments hereto is by the QuoVadis PMA. Amendments may be made by updating this entire document or by addendum. The QuoVadis PMA, at its sole discretion, determines whether changes to this CP/CPS require notice or any change in the OID of a Certificate issued pursuant to this CP/CPS.

1.6 Definitions and Acronyms

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

Application Software Suppliers: Mean those developers of Internet browser software or other software that displays or uses certificates and distribute Root Certificates embedded in their software, including but not limited to Apple Inc., Microsoft Corporation, Mozilla Corporation, Adobe Systems Incorporated, Oracle Corporation, etc.

Authority Letter: The Authority Letter is a signed by a Confirming Person acting for the Applicant for EV Certificates to establish the authority of individuals to act as the Certificate Holder's agents.

Certificate Approver: A Certificate Approver is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorise other employees or third parties to act as a Certificate Requesters, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certificate Application: Any of several forms completed by Applicant or QuoVadis and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

Certificate Holder: Means either the Individual to whom an end entity Certificate is issued, referred to as a Registrant in the Trust/Link system or the Individual responsible for requesting, installing and maintaining the trusted system for which an TLS/SSL Certificate has been issued, referred to as a Subscriber in the Trust/Link system.

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

Certificate Requester: A Certificate Requester is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company), and who completes and submits a Certificate Request on behalf of the Applicant.

Confirming Person: A confirming Person is a natural person who must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) who has express authority to sign the QV Authority Letter on behalf of the Applicant.

Contract Signer: A Contract Signer is a natural person who is employed by the Applicant and who has express authority to sign Certificate Holder Agreements on behalf of the Applicant.

Effective Date: Is the date that the Baseline Requirements v1.0 come into force, which is 1 July 2012.

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Participants: A Participant is an individual or entity within the QuoVadis PKI and may include: CAs and their Subsidiaries and Holding Companies; Certificate Holders including Applicants; and Relying Parties.

Qualified Certificate: A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the qualification requirements defined by the applicable legal framework of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS Regulation”).

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using the QuoVadis Repository.

Repository: The Repository refers to the CRL, OCSP, and other directory services provided by QuoVadis containing issued and revoked Certificates.

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.

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

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
PMA	QuoVadis Policy Management Authority
EV	Extended Validation
FIPS	Federal Information Processing Standard
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ERA	Enterprise Registration Authority
LRA	Local Registration Authority
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2 Publication and Repository Responsibilities

2.1 Repositories

The QuoVadis Repository (https://www.quovadisglobal.com/repository) serves as the primary repository for revocation data on issued Certificates. However, copies of QuoVadis directories may be published at such other locations as required for efficient operation of the QuoVadis PKI.

2.2 Publication of Certificate Information

QuoVadis operates and maintains its Repository with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the Certificates issued by its CAs.

QuoVadis publishes Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) resources to allow Relying Parties to determine the validity of a QuoVadis Certificate. Each CRL contains entries for all revoked un-expired Certificates issued. QuoVadis maintains revocation entries on its CRLs, or makes Certificate status information available via OCSP, until after the expiration date of the revoked Certificate.

To ensure TLS/SSL Certificates function properly throughout their lifecycle, QuoVadis may log TLS/SSL Certificates with a Certificate Transparency database ("CT Log"). CT Log information is publicly accessible. Once submitted, Certificate information cannot be removed from a CT Log.

QuoVadis conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates ("Baseline Requirements") published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

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

QuoVadis conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates ("Code Signing Minimum Requirements") published at https://aka.ms/csbr. In the event of any inconsistency between this document and those Requirements, those Requirements

take precedence over this document. The CA/Browser Forum reserved policy identifier 2.23.140.1.4.1 is included in QuoVadis code signing certificates to assert compliance with the Code Signing Minimum Requirements. The QuoVadis Code Signing OID (1.3.6.1.4.1.8024.0.2.200.1.1) is also included in code signing certificates.

2.3 Time or Frequency of Publication

QuoVadis issues a new CRL at least every twelve (12) hours and prior to the expiration of the current CRL. QuoVadis also provides an OCSP resource that is updated at least every twelve (12) hours. Certificate information is published promptly following generation and issue, and within 20 minutes of revocation.

2.4 Access Controls on Repositories

Participants (including Certificate Holders and Relying Parties) accessing the QuoVadis Repository and other QuoVadis directory resources are deemed to have agreed with the provisions of this CP/CPS and any other conditions of usage that QuoVadis may make available. Participants demonstrate acceptance of the conditions of usage of this CP/CPS by using a QuoVadis Certificate. Failure to comply with the conditions of usage of the QuoVadis Repository and web site may result in termination of the relationship between QuoVadis and the party, at QuoVadis' sole discretion, and any unauthorised reliance on a Certificate shall be at that party's risk. QuoVadis is the only entity that has write access to Repositories.

3 Identification and Authentication

The identification and authentication procedures used by QuoVadis depend on the class of Certificate being issued. See Appendix B for Certificate Profiles and the relevant verification requirements.

3.1 Naming

3.1.1 Types Of Names

All Certificate Holders 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 Certificate Holder. 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 contain provisions prohibiting 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, when applicable, the Subject Alternative Name extension.

3.1.2 Need For Names To Be Meaningful

Distinguished names must be meaningful, unambiguous, and unique. QuoVadis ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field accurately identify the legal entity that is the subject of the Certificate. Similarly, QuoVadis uses non-ambiguous designations in the Issuer field to identify itself as the Issuer of a Certificate (e.g., QuoVadis Global SSL CA).

3.1.3 Pseudonymous Certificate Holders

QuoVadis does not issue anonymous or pseudonymous Certificates.

3.1.4 Rules For Interpreting Various Name Forms

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references. In addition, see the Certificate Profiles detailed in Appendix B.

3.1.5 Uniqueness Of Names

Name uniqueness is ensured through the use of the Common Name attribute of the Subject Field, which contains the authenticated domain name, which is controlled under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication, And Role Of Trademarks

Certificate Holders shall solely be responsible for the legality of the information they present for use in Certificates issued under this CP/CPS in any jurisdiction in which such content may be used or viewed. Certificate Holders represent and warrant that when submitting Certificate Requests to QuoVadis and using a domain and distinguished name (and all other Certificate Application information) they do not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, or to confuse or mislead any person, whether natural or corporate. Certificate Holders shall defend, indemnify, and hold QuoVadis harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions against QuoVadis.

3.2 Initial Identity Validation

3.2.1 Method To Prove Possession Of Private Key

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

3.2.2 Authentication Of Organisation Identity

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

3.2.2.1 Validation of Domain Authorization 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:

1. 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)
2. Communicating directly with the Domain Name Registrant by calling their phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The phone number used must be the number listed by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.3;
3. Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorization Domain Name. Performed in accordance with BR section 3.2.2.4.4;
4. 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 3.2.2.4.6;
5. Confirming the Applicant's control over the requested Authorization Domain Name (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;
6. 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;
7. 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;
8. 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 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13;
9. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14;
10. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; and
11. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to

validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.

High Risk Domains

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

3.2.2.2 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:

1. 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;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
4. After July 31, 2019, QuoVadis will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
7. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

3.2.2.3 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, QuoVadis programmatically enforces that the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”.

3.2.2.4 Data Source Accuracy

Prior to using a data source as a Reliable Data Source, QuoVadis evaluates it for reliability, accuracy and resistance to falsification.

3.2.3 Authentication Of Individual Identity

Where applicable, authentication of Individual identity is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B. TLS/SSL certificates are only issued to Organisations and not natural persons.

3.2.4 Non-Verified Certificate Holder Information

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

3.2.5 Validation Of Authority

Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

For Certificates issued at the request of a Certificate Holder's Agent, both the Agent and the Certificate Holder shall jointly and severally indemnify and hold harmless QuoVadis, and its parent companies, subsidiaries, directors, officers, and employees. The Certificate Holder shall control and be responsible for the data that an Agent of the Certificate Holder supplies to QuoVadis. The Certificate Holder must promptly notify QuoVadis of any misrepresentations and omissions made by an Agent of the Certificate Holder.

3.3 Identification And Authentication For Re-Key Requests

3.3.1 Identification And Authentication For Routine Re-Key

Identification and Authentication procedures are the same for re-key as for a new application. Key pairs must always expire at the same time as the associated Certificate.

3.3.2 Identification and Authentication For Re-Key After Revocation

After revocation, a Certificate Holder must submit a new application.

3.4 Identification and Authentication For Revocation Requests

See Section 4.9 for information about Certificate Revocation procedures.

4 Certificate Life-Cycle Operation Requirements

4.1 Certificate Application

The process to apply for QuoVadis Certificates varies by Certificate Policy and is described in Appendix B.

4.2 Certificate Application Processing

4.2.1 Performing Identification And Authentication Functions

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

4.2.2 Approval Or Rejection Of Certificate Applications

From time to time, QuoVadis may modify the requirements related to application information requested, based on QuoVadis requirements, business context of the usage of Certificates, or as may be required by law, or changes to the EV Guidelines, Baseline Requirements, or the Code Signing Minimum Requirements.

QuoVadis, in its sole discretion, may refuse to accept an application for a Certificate or for the renewal of a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. QuoVadis reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3 Time To Process Certificate Applications

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

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

4.2.4 Certificate Authority Authorisation (CAA)

Prior to issuing TLS/SSL Digital Certificates, QuoVadis checks for CAA records for each dNSName in the subjectAltName extension of the Digital Certificate to be issued. If the QuoVadis Digital Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, QuoVadis processes the issue, issuewild, and iodef property tags as specified in RFC 6844 as amended by Errata 5065 (Appendix A). QuoVadis may not act on the contents of the iodef property tag. QuoVadis will not issue a Digital Certificate if an unrecognized property is found with the critical flag.

QuoVadis may not check CAA records for the following exceptions:

I. For Digital Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
II. For Digital Certificates issued by a Technically Constrained Subordinate CA Certificate, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
III. If the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

QuoVadis treats a record lookup failure as permission to issue if:

I. the failure is outside the CA's infrastructure;
II. the lookup has been retried at least once; and
III. the domain's zone does not have a DNSSEC validation chain to the ICANN root.

QuoVadis documents potential issuances that were prevented by a CAA record, and will dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. QuoVadis support mailto: and https: URL schemes in the iodef record.

The identifying CAA domain for QuoVadis is ‘quovadisglobal.com’.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificate issuance is governed by the practices described in and any requirements imposed by this CP/CPS.

4.3.2 Notification To Certificate Holder By The CA Of Issuance Of Certificate

Certificates are delivered to the Certificate Requester designated in the Certificate Application.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

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

BY ACCEPTING A CERTIFICATE, THE CERTIFICATE HOLDER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE CERTIFICATE HOLDER AGREEMENT. BY ACCEPTING A CERTIFICATE, THE CERTIFICATE HOLDER 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

All Certificates issued within the QuoVadis PKI are made available in public repositories except where the Certificate Holder has requested that the Certificate not be published.

4.5 Key Pair And Certificate Usage

4.5.1 Certificate Holder Private Key And Certificate Usage

Certificate Holders shall protect their private keys from access by unauthorised personnel or other third parties. Certificate Holders shall use private keys only in accordance with the usages specified in the key usage field extension.

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 by querying the existence or validity of, or by seeking to place or by placing reliance upon, on a Certificate.

QuoVadis assumes that all user software will be compliant with X.509, the TLS/SSL protocol, and other applicable standards that enforce the requirements and requirements set forth in this CP/CPS. QuoVadis does not warrant that any third party's software will support or enforce such controls or requirements, and all Relying Parties are advised to seek appropriate technical or legal advice.

Parties relying on a Certificate must adhere to the TLS/SSL protocol and verify a digital signature at all times by checking the validity of the associated Certificate against the relevant CRL or OCSP resource provided by QuoVadis. Relying on an unverifiable digital signature or TLS/SSL session may result in risks that the Relying Party assumes in whole and which QuoVadis does not assume in any way.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS;
- That the Certificate is being used in accordance with its key usage field extensions specified in this CP/CPS and contained in the Certificate; and
- That the Certificate is valid at the time of reliance by reference to the QuoVadis CRL or OCSP and the Certificate has not been revoked.

Warranties are only valid if the steps detailed above have been carried out.

4.6 Certificate Renewal

Renewal of a Certificate means reissuance of the Certificate using the same key pair. QuoVadis does not support Renewal; key pairs must always expire at the same time as the associated Certificate. QuoVadis makes reasonable efforts to notify Certificate Holders of the imminent expiration of a Certificate. Identification and Authentication procedures are generally the same for replacement Certificates as for a new application.

4.7 Certificate Re-Key

Re-keying a Certificate means to request a new Certificate with the same contents except for a new key pair. Identification and Authentication procedures are the same for re-key as for a new application.

4.8 Certificate Modification

QuoVadis may reissue or replace a valid Certificate when the Certificate Holder's common name, organization name, device name, or geographic location changes.

Modified information must undergo the same Identification and Authentication procedures as for a new Certificate.

4.9 Certificate Revocation And Suspension

4.9.1 Circumstances For Revocation

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. QuoVadis may revoke any Certificate at its sole discretion or based on information confirmed in a Certificate Problem Report. QuoVadis will revoke a Certificate if:

- QuoVadis determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Certificate Holder requests in writing the revocation of their Certificate;
- The Certificate Holder indicates that the original Certificate Request was not authorised and does not retroactively grant authorization;
- QuoVadis obtains reasonable evidence that there has been loss, theft, modification, unauthorised disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate, or that the Certificate has otherwise been misused;
- QuoVadis receives notice or otherwise becomes aware that a Certificate Holder has breached a material obligation under the Certificate Holder Agreement or other contractual obligations;
- QuoVadis receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
- QuoVadis is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP 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 Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- QuoVadis is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- QuoVadis determines, in its sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or QuoVadis' CP/CPS;
- QuoVadis receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Certificate Holder that is contained within the Certificate;

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

4.9.2 Who Can Request Revocation

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

Parties who are not the Certificate Holder (such as Relying Parties, Application Software Suppliers, and other third parties) may file a Certificate Problem Report to initiate a Certificate revocation request. Problem reports may include complaints; suspected Private Key compromise; Certificate misuse, including Code Signing

Certificates used to sign Suspect Code; or other types of fraud, compromise, misuse, or inappropriate conduct related to the Certificate.

4.9.3 Procedure For Revocation Request

QuoVadis will revoke a Certificate upon receipt of a valid request from the Certificate Holder, verified through an out- of-band communication. QuoVadis will begin an investigation of all Certificate Problem Reports within twenty-four

hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

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

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

Certificate Holders may also revoke their Certificates via the Trust/Link system.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which The CA Must Process The Revocation Request

QuoVadis will begin investigation of a certificate problem report within 24 hours of its receipt. QuoVadis will take commercially reasonable steps to revoke the Digital Certificate within 4 hours of receipt of a valid revocation request.

In the case of Code Signing Certificates, QuoVadis complies with the revocation timeframes specified for malware in section 13.1.5.3 of Code Signing Minimum Requirements.

4.9.6 Revocation Checking Requirement For Relying Parties

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

4.9.7 CRL Issuance Frequency

QuoVadis uses its offline root CAs to publish CRLs for its subordinate CAs at least every 6 months and within 24 hours after revoking a subordinate CA certificate. All other CRLs are published at least every 24 hours. CRLs are published and are available 24 hours a day, 7 days a week.

4.9.8 Maximum Latency For CRL

The maximum latency for the CRL is 10 minutes.

4.9.9 On-Line Revocation/Status Checking Availability

QuoVadis provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of the Certificate.

4.9.10 On-Line Revocation Checking Requirement

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

QuoVadis supports an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements.

Where required by the Baseline Requirements (all TLS/SSL certificates) or other industry requirements, if the QuoVadis OCSP responder receives a request for status of a certificate that has not been issued, then the responder will not respond with a "good" status.

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements for Key Compromise

QuoVadis will use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that a

CA's private key has been compromised.

4.9.13 Circumstances For Suspension

The QuoVadis PKI does not support suspension of Certificates.

4.9.14 Who Can Request Suspension

The QuoVadis PKI does not support suspension of Certificates.

4.9.15 Procedure For Suspension Request

The QuoVadis PKI does not support suspension of Certificates.

4.9.16 Limits On Suspension Period

The QuoVadis PKI does not support suspension of Certificates.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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.

4.10.2 Service Availability

Digital Certificate status services are available 24 hours a day, 7 days a week, 365 days of the year.

4.11 End Of Subscription

A Certificate Holder may terminate its subscription to the QuoVadis PKI by allowing a Certificate or applicable agreement to expire without renewal, or by voluntarily revoking a Certificate.

4.12 Key Escrow And Recovery

The QuoVadis PKI does not support key escrow or recovery of Certificate Holder private keys.

5 Facility, Management, and Operational Controls

The section of the CP/CPS provides a high level description of the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by QuoVadis to provide trustworthy and reliable CA operations. 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 unauthorized 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 operations from a secure datacentre located in Hamilton, Bermuda. The datacentre is a purpose-built steel and composite compartment, with raised floor construction and an array of resilient security and environmental systems. QuoVadis operates under a security policy designed to deter, prevent and detect unauthorized access to the datacentre.

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

The QuoVadis secure operating area is connected to dual power feeds via a fault tolerant design. All critical components are connected to dual uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure. In the event of a power failure there is an automatic failover to a standby generator.

5.1.4 Water Exposures

The QuoVadis secure operating area provides protection against water. It is located on an upper floor with raised flooring, floors and walls are sealed.

5.1.5 Fire Prevention And Protection

The QuoVadis secure datacentre provides protection against fire and contains with an automatic FM200 extinguishing system.

5.1.6 Media Storage

All magnetic media containing QuoVadis PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the QuoVadis service operations area or in a secure off-site storage area.

5.1.7 Waste Disposal

Paper documents and magnetic media containing QuoVadis PKI information or confidential information are securely disposed of by:

- in the case of magnetic media: physical damage to or complete destruction of the asset; or the use of an approved utility to wipe or overwrite magnetic media; or
- in the case of printed material, shredding or destruction by an approved service.

5.1.8 Off-Site Backup

An offsite location is used for the storage and retention of backup software and data. The off site storage is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e. software and data are stored in fire-rated safes and containers which are located behind access-controlled doors in areas accessible only by authorised personnel).

5.2 Procedural Controls

Administrative processes are described in detail in the various documents used within and supporting the QuoVadis PKI. Administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms,

are maintained in accordance with this CP/CPS and other relevant operational documents. Except for certain RA functions described in this CP/CPS, QuoVadis does not outsource operations associated with Root CA2.

5.2.1 Trusted Roles

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

5.2.2 Number Of Persons Required Per Task

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

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

5.2.3 Identification And Authentication For Each Role

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

5.2.4 Roles Requiring Separation Of Duties

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, And Clearance Requirements

Background checks are conducted on all individuals selected to take up a trusted role in the QuoVadis PKI in accordance with a designated security screening procedure, prior to the commencement of their duties.

For purposes of mitigating the risk that one individual acting alone could compromise the integrity of the QuoVadis PKI or any Certificate issued therein, QuoVadis performs relevant background checks of individuals and defines the tasks that the individuals will be responsible to perform. QuoVadis determines the nature and extent of any background checks in its sole discretion. The foregoing fully stipulates QuoVadis' obligations with respect to personnel controls and QuoVadis shall have no other duty or responsibility with respect to the foregoing. Without limitation, QuoVadis shall not be liable for employee conduct that is outside of their duties and for which QuoVadis has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.2 Background Check Procedures

Background check procedures may include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Criminal records
- Credit/financial history and status
- Driving licenses
- Social security records

Where the above checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, QuoVadis will utilise available substitute investigation techniques permitted by law that provide similar information including background checks performed by applicable government agencies.

5.3.3 Training Requirements

QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities. This includes specific vetting training for Validation Specialists, who may not undertake

Certificate validation and issuance until they have passed a suitable examination on knowledge and skills.

5.3.4 Retraining Frequency And Requirements

Validation Specialists engaged in Certificate validation and issuance must maintain adequate skill levels in order to have issuance privilege, consistent with QuoVadis' training and performance programs.

5.3.5 Job Rotation Frequency And Sequence

QuoVadis provides and maintains a program of job rotation in order to maintain appropriate and required levels of competency across key roles.

5.3.6 Sanctions For Unauthorised Actions

Appropriate disciplinary actions are taken for unauthorised actions.

5.3.7 Independent Contractor Requirements

The QuoVadis PKI does not support the use of independent contractors to fulfil trusted roles.

5.3.8 Documentation Supplied To Personnel

QuoVadis provides personnel all required training materials needed to perform their job function and their duties under the job rotation program. This includes specific documentation of the validation, issuance, and revocation processes for Certificates.

5.4 Audit Logging Procedures

5.4.1 Types Of Events Recorded

QuoVadis records details of the actions taken to process a certificate request and to issue a Digital Certificate, including all information generated and documentation received in connection with the certificate request. QuoVadis logs the following events:

- CA key lifecycle management events;
- 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 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 Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5 Audit Log Backup Procedures

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

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 undergoes periodic penetration tests conducted by an external third party. QuoVadis also performs internal vulnerability assessments on a regular basis.

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) Certificate Holder Agreements;
- Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- CRL lists posted; and
- Audit Opinions as discussed in this QuoVadis CP/CPS.

5.5.2 Retention Period For Archive

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 Protection Of Archive

Archives shall be retained and protected against modification or destruction.

5.5.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5 Requirements For Time-Stamping Of Records

QuoVadis supports time stamping of all of its records. All events that are recorded within the QuoVadis service include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis PKI rely on a trusted time source.

5.5.6 Archive Collection System

The QuoVadis Archive Collection System is internal.

5.5.7 Procedures To Obtain And Verify Archive Information

Only Issuing CA officers 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 Key Changeover

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 associated with that key. A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active.

5.7 Compromise And Disaster Recovery

QuoVadis has an Incident Response Plan as well as a Business Continuity Plan. The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by fire, strikes, or other crisis events.

QuoVadis has in place business resumption procedures that provide for the immediate continuation of Certificate revocation services in the event of an unexpected

emergency. QuoVadis regards its disaster recovery and business resumption plan as proprietary and it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.

QuoVadis has in place an appropriate key compromise plan detailing its activities in the event of a compromise of an Issuing CA private key. This plan includes procedures for:

- Revoking all Certificates signed with that Issuing CA's private key;
- Promptly notifying all Certificate Holders with Certificates issued by that Issuing CA; and
- Generating a new key pair and signing a new CA Certificate.

5.7.1 QuoVadis Business Continuity Plan

The QuoVadis Business Continuity Plan is strictly confidential and provides for:

- Incident and compromise handling procedures;
- Computing resources, software, and/or corrupted data handling procedures;
- Entity private key compromise procedures; and
- Entity public key revocation procedures; and
- Business continuity capabilities and procedures after a disaster.

5.8 CA And/Or RA Termination

In case of termination of CA operations, QuoVadis will provide timely notice and transfer of responsibilities to succeeding entities. Before terminating its own CA activities, QuoVadis will where possible take the following steps:

- Give timely notice of revocation to each affected Certificate Holder.
- Revoke all Certificates that are still un-revoked or un-expired at the end of the notice period without seeking Certificate Holder's consent.
- Make reasonable arrangements to preserve its records according to this CP/CPS.
- Reserve its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary standards.
- Notify relevant government and accreditation bodies under applicable laws and related regulations or standards.

Upon termination of a CA, QuoVadis personnel shall destroy the CA private key by deleting, overwriting, or physical destruction.

6 Technical Security Controls

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

Root CA key pair generation is witnessed by a Qualified Auditor and follows a formal key generation script. In all instances, CA private keys are generated in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the QuoVadis environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple members of the QuoVadis management team. Such allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

6.1.2 Private Key Delivery To Certificate Holder

Certificate Holders are solely responsible for the generation of the private keys used in their Certificate Requests. QuoVadis does not provide TLS/SSL key generation, escrow, recovery or backup facilities.

6.1.3 Public Key Delivery To Certificate Issuer

Upon making a Certificate Application, the Certificate Holder is solely responsible for generating an RSA key pair and submitting it to QuoVadis in the form of a PKCS#10 CSR. Certificate requests are generated using the key generation facilities available in the Certificate Holder's web server software.

6.1.4 Certification Authority Public Key To Relying Parties

QuoVadis public keys are securely delivered to software providers to serve as trust anchors in commercial browsers and operating system root stores, or may be specified in a Certificate validation or path discovery policy file. Relying Parties may also obtain QuoVadis self-signed CA Certificates containing its public key from the QuoVadis web site.

6.1.5 Key Sizes

Key lengths within the QuoVadis PKI are determined by the QuoVadis Policy Management Authority in accordance with industry guidance and best practice. Key sizes for individual certificate profiles are disclosed in Appendix A and Appendix B. The

QuoVadis Issuing CA uses an RSA minimum key length of 2048-bit modulus. Certificate Holders may submit 2048-bit or larger keys to QuoVadis.

6.1.6 Public Key Parameters Generation And Quality Checking

The cryptographic modules used by QuoVadis have been validated to conforming to FIPS 140-2 Level-3 and provide random number generation and on-board creation of suitable key lengths for RSA public key generation.

QuoVadis programmatically checks key size, public exponent range and modulus of incoming public key parameters against regulatory requirements and industry best practices.

6.1.7 Key Usage Purposes (As Per X.509 V3 Key Usage Field)

Private Keys corresponding to QuoVadis Root Certificates are not used to sign Certificates except in the following cases:

I. Self-signed Certificates to represent the QuoVadis Root CA itself;
II. Certificates for Subordinate CAs and Cross Certificates; and
III. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates);

QuoVadis CA Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and also to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of QuoVadis. Key usages are specified in the Certificate Profiles in Appendix A and B.

6.2 Private Key Protection And Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards And Controls

The cryptographic modules used by the QuoVadis PKI are validated to provide FIPS 140-2 Level-3 security standards in both the generation and the maintenance in all Root and Issuing CA private keys.

6.2.2 Private Key (N Out Of M) Multi-Person Control

Subject to the requirements of the CP/CPS, the QuoVadis PKI uses trusted multi-person control for both access control and authorisation control.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

Issuing CA private keys are stored in an encrypted state (using an encryption key to create a “cryptographic wrapper” around the key. Access is only by N-of-M control as defined in this CP/CPS. Backup copies are maintained on site and in secure, offsite storage.

6.2.5 Private Key Archive

The QuoVadis PKI does not support private key archive.

6.2.6 Private Key Transfer Into Or From A Cryptographic Module

If a Cryptographic Module is used, the Private Key must be generated in it and remain there in encrypted form, and be decrypted only at the time at which it is being used. Private Keys must never exist in plain-text form outside the cryptographic module. In the event that a Private Key is to be transported from one Cryptographic Module to another, the Private Key must be encrypted during transport.

6.2.7 Private Key Storage On Cryptographic Module

CA private keys are generated and stored in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3.

6.2.8 Method Of Activating Private Key

An authorised user must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

Certificate Holders are solely responsible for protection of their private keys. QuoVadis maintains no involvement in the generation, protection, or distribution of such keys. QuoVadis suggests that Certificate Holders use a strong password or equivalent authentication method to prevent unauthorised access and usage of the Certificate Holder private key.

6.2.9 Method Of Deactivating Private Key

Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorised access. After use, they must be deactivated using, for example, a manual logout procedure or a passive timeout. When not in use, cryptographic modules should be removed and securely stored, unless they are within the sole control of an authorised user.

Certificate Holders should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10 Method Of Destroying Private Key

Private keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked.

All Digital Certificate Holders have an obligation to protect their private keys from compromise. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure or unauthorised use.

Upon expiration of a key pair's allowed lifetime, or upon CA termination, QuoVadis personnel shall destroy the CA private key by deleting and overwriting the data (e.g., via re-initialization or zeroization) or physical destruction (e.g., with a metal shredder or hammer). Such destruction shall be documented.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by the QuoVadis PKI are validated to FIPS 140-2 Level-3 security standards.

6.3 Other Aspects Of Key Pair Management

6.3.1 Public Key Archival

Public keys will be recorded in Certificates that will be archived in the Repository. No separate archive of public keys will be maintained. The validity period of Certificates will be dependent on the Certificate Policy in question.

6.3.2 Certificate Operational Periods And Key Pair Usage Periods

The maximum validity periods for Certificates issued within the QuoVadis PKI are:

Root CA Certificate 30 years
Issuing CA Certificates 10-15 years
Business SSL Certificates 3 years (825 days after March 1, 2018)
EV SSL Certificates 2 years

6.4 Activation Data

6.4.1 Activation Data Generation And Installation

Two-factor authentication shall be used to protect access to a private key. One of these factors must be randomly and automatically generated.

6.4.2 Activation Data Protection

No activation data other than access control mechanisms is required to operate cryptographic modules. Personal Identification Codes 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. Activation data should be memorized, not written down. Activation data must never be shared. Activation data must not contain the user's personal information.

6.4.3 Other Aspects Of Activation Data

No stipulation.

6.5 Computer Security Controls

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

6.5.1 Specific Computer Security Technical Requirements

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

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

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

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

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

6.6.1 System Development Controls

Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2 Security Management Controls

Formal procedures and controls are in place to relating to the security-related configurations of QuoVadis' CA systems.

6.6.3 Life Cycle Security Controls

QuoVadis employs a configuration management methodology for the installation and ongoing maintenance of the CA systems. The CA software, when first loaded, provides a method for QuoVadis to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

The QuoVadis Chief Security Officer periodically verifies the integrity of the CA software and monitors the configuration of the CA systems.

6.7 Network Security Controls

All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits

services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

All unused network ports and services on Issuing CA equipment are turned off to provide protection against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone (offline) configurations.

6.8 Time-Stamping

See Section 5.5.5. In addition, QuoVadis provides a Time-Stamp Authority (TSA) service for use with specific QuoVadis products such as Code Signing Certificates.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Numbers

Information for interpreting Certificate and CRL Profiles may be found in IETF RFC 5280. QuoVadis Certificates follow the ITU X.509v3 standard, which allows a CA to add certain Certificate extensions to the basic Certificate structure.

7.1.2 Certificate Extensions

See Appendix A and Appendix B.

7.1.3 Algorithm Object Identifiers

See Appendix A and Appendix B.

7.1.4 Name Forms

See Appendix A and Appendix B.

7.1.5 Name Constraints

Effective August 16, 2017 QuoVadis no longer accepts new external entities who wish to operate their own TLS/SSL CAs as subordinate CAs under a QuoVadis root.

Legacy external TLS/SSL root signings are either Technically Constrained or publicly disclosed and audited. Technically Constrained CA certificates include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for including the id-kp-serverAuth extended key usage and include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryNames.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a CP/CPS such as this. The Certificate Policy OIDs that incorporate this CP/CPS into a given Certificate by reference (and identify that this CP/CPS applies to a given Certificate containing the OID) are listed in Appendix A and Appendix B.

7.1.7 Usage Of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax And Semantics

QuoVadis Certificates include a brief statement in the Policy Qualifier field of the Certificate Policy extension to inform potential Relying Parties on notice of the limitations of liability and other terms and conditions on the use of the Certificate, including those contained in this CP/CPS, which are incorporated by reference into the Certificate.

7.1.9 Processing Semantics For The Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number

QuoVadis issues version 2 CRLs conforming to RFC 5280, and which contain the basic fields listed below:

- Version
- Issuer Signature Algorithm
- Issuer Distinguished Name
- thisUpdate (UTC format)
- nextUpdate (UTC format – thisUpdate plus 12 hours)
- Revoked Certificates list
- Serial Number
- Revocation Date (see CRL entry extension for Reason Code below)
- Issuer's Signature

7.2.2 CRL And CRL Entry Extensions

- CRL Number (monotonically increasing integer - never repeated)
- Authority Key Identifier (same as Authority Key Identifier in Certificates issued by CA)
- CRL Entry Extensions
  - Invalidity Date (UTC - optional)

- Reason Code (optional)

7.3 Online Certificate Status Protocol Profile

OCSP is enabled for all Certificates within the QuoVadis PKI.

7.3.1 Online Certificate Status Protocol Version Numbers

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

7.3.2 Online Certificate Status Protocol Extensions

No Stipulation.

7.4 Certificate Transparency

QuoVadis Certificates MAY include two or more Signed Certificate Timestamps (SCT) from independent Certificate Transparency Logs. Information on Certificate Transparency may be found in IETF RFC 6962

8 Compliance Audit and Other Assessments

8.1 Frequency, Circumstance And Standards Of Assessment

The practices specified in this CP/CPS have been designed to meet or exceed the requirements of, and QuoVadis is audited for compliance to, generally accepted and developing industry standards including:

- AICPA/CICA WebTrust for Certification Authorities, WebTrust for Baseline Requirements and the WebTrust Extended Validation Program;
- Bermuda Authorised Certification Service Provider standards of the Bermuda electronic Transactions Act;
- Swiss Zert ES Qualified Certification Service Provider standards (ZertES), including adherence to relevant ETSI standards and other specifications

8.2 Identity And Qualifications Of Assessor

The audit services described in Section 8.1 are performed by independent, recognised, credible, and established audit firms having significant experience with PKI and cryptographic technologies. The WebTrust and Bermuda Certificate Service Provider audits have been carried out by Ernst & Young. The accreditation audits for Swiss and ETSI requirements have been performed by KPMG AG.

8.3 Assessor's Relationship To Assessed Entity

QuoVadis and the auditors do not have any other relationship that would impair their independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social, or other relationships that could result in a conflict of interest.

8.4 Topics Covered By Assessment

Topics covered by the annual audits of QuoVadis include but are not limited to CA business practices disclosure (i.e., this CP/CPS), the service integrity of QuoVadis' CA operations, the environmental controls that QuoVadis implements to ensure trustworthy systems, and QuoVadis' compliance with relevant laws, regulations, and guidelines.

8.5 Actions Taken As A Result Of Deficiency

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by QuoVadis with input from auditors. QuoVadis at its sole discretion will determine an appropriate course of action and time frame to rectify the deficiency.

8.6 Publication Of Audit Results

The results of these audits in the form of publicly available audit reports or opinions as provided by the external auditors responsible for these audits are published on the QuoVadis website at https://www.quovadisglobal.com/accreditations.aspx or are available upon request.

8.7 Self Audits

QuoVadis controls service quality by performing quarterly self-audits against a randomly selected sample of Certificates being no less than three percent of the certificates issued.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance Or Renewal Fees

QuoVadis charges Certificate Holder fees for verification, issuance, and renewal. Such fees are detailed on the QuoVadis web site. QuoVadis retains its right to effect changes to such fees. QuoVadis customers will be suitably advised of price amendments as detailed in relevant customer agreements.

9.1.2 Certificate Access Fees

QuoVadis reserves the right to establish and charge a reasonable fee for access to its Repository.

9.1.3 Revocation Or Status Information Access Fees

QuoVadis does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of a QuoVadis issued Certificate through the use of CRLs. QuoVadis reserves the right to establish and charge a reasonable fee for providing Certificate status information services via OCSP.

9.1.4 Fees For Other Services

No stipulation.

9.1.5 Refund Policy

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

9.2 Financial Responsibilities

9.2.1 Financial Records

QuoVadis is responsible for maintaining its financial books and records in a commercially reasonable manner and shall engage the services of an independent accounting firm to provide financial services, including periodic audits.

9.2.2 No Partnership or Agency

Certificate Holder shall not represent itself as being the affiliate nor an agent, partner, employee or representative of QuoVadis and shall not hold itself out as such nor as having any power or authority to incur any obligation of any nature express or implied on behalf of QuoVadis and nothing in this Agreement shall operate nor be construed so as to constitute Certificate Holder as an agent, partner, employee, or representative of QuoVadis.

9.2.3 Insurance Cover

QuoVadis maintains the following insurance related to its respective performance and obligations:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

9.2.4 Other Assets

No stipulation.

9.2.5 Insurance Or Warranty Coverage For End-Entities

Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the private key that corresponds to the public key in their QuoVadis Certificate. Relying Parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.3 Confidentiality Of Business Information

9.3.1 Scope Of Confidential Information

QuoVadis keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys;
- Any activation data used to access private keys or gain access to the CA system;

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

9.3.2 Information Not Within The Scope Of Confidential Information

Information appearing in Certificates or stored in the Repository is considered public and not within the scope of confidential information, unless statutes or special agreements so dictate.

9.4 Responsibility To Protect Private Information

All Participants in the QuoVadis PKI QuoVadis and all others using or accessing any personal data in connection with matters dealt with this CP/CPS shall comply with the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amending and/or implementing legislation enacted from time to time, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. QuoVadis complies with the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9.4.1 Privacy Plan

QuoVadis has implemented a privacy policy in compliance with this CP/CPS. The QuoVadis privacy policy is published on the QuoVadis web site.

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.

9.4.3 Information Deemed Not Private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private. This QuoVadis CP/CPS is a public document and is not confidential information and is not treated as private.

9.4.4 Responsibility To Protect Private Information

Information supplied to QuoVadis as a result of the practices described in this CP/CPS may be covered by national government or other privacy legislation or guidelines. QuoVadis will not divulge any private personal information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

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 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 accessible directories and be communicated to others.

9.4.6 Disclosure Pursuant To Judicial Or Administrative Process

As a general principle, no document or record belonging to QuoVadis is released to law enforcement agencies, officials, or persons relating to civil discovery proceedings except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to QuoVadis to be under appeal when served on QuoVadis (QuoVadis being under no obligation to determine the same), and which has been determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable.

9.5 Intellectual Property Rights

All Intellectual Property Rights including all copyright in all Certificates and all documents (electronic or otherwise) belong to and will remain the property of QuoVadis.

Certificates are the exclusive property of QuoVadis. QuoVadis gives permission to reproduce and distribute Certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. QuoVadis reserves the right to revoke a Certificate at any time and at its sole discretion. Private keys and public keys are the property of the applicable Certificate Holders who rightfully issue and hold them.

This QuoVadis CP/CPS and the Proprietary Marks are the intellectual property of QuoVadis. QuoVadis retains exclusive title to, copyright in, and the right to license this

QuoVadis CP/CPS. QuoVadis excludes all liability for breach of any other intellectual property rights.

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 Certificate Holder Agreement;
- All Relying Parties who reasonably rely on a Valid Certificate; and
- All Application Software Suppliers with whom QuoVadis has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier.

QuoVadis discharges its obligations by:

- Providing the operational infrastructure and certification services, including the Repository, OCSP responders and CRLs;
- Making reasonable efforts to ensure it conducts and efficient and trustworthy operation;
- Maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation; and
- Investigating any suspected compromise which may threaten the integrity of the QuoVadis PKI.

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 that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

QuoVadis makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

9.6.2 Third Party LRA Representations and Warranties

Third party LRAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to, or which reasonably ought to be known to, the LRA or its agents;
- There are no errors in the information in the Certificate that were introduced by the LRA or its agents as a result of a failure to exercise reasonable care; and
- Their Certificates meet all material requirements of this CP/CPS.

Additional representations and warranties relevant to LRAs may be included in Certificate Holder Agreements for specific Certificate Policies.

9.6.3 Certificate Holder Representations And Warranties

As part of the Certificate Holder Agreement agreed to by all Certificate Holders, the following commitments and warranties are made for the express benefit of QuoVadis and all Relying Parties and Application Software Suppliers:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to QuoVadis, both in the Certificate Request and as otherwise requested by QuoVadis in connection with the issuance of the Certificate(s) to be supplied by QuoVadis;
- Protection of Private Key: An obligation and warranty by the Certificate Holder or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated access information or device such as a password or token);
- Acceptance of Certificate: An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate;
- Use of Certificate: An obligation and warranty to:
  - Server Certificates: install the Certificate only on the server accessible at the domain name listed on the Certificate,
  - Code Signing Certificates: not use the Certificate to digitally sign hostile code, spyware or other malicious software (or to disable antispyware and other protective measures or provide false or misleading descriptions of the signed code's functions or features), and to use the Certificate solely in compliance with all applicable laws, solely for authorised company business and solely in accordance with the Certificate Holder Agreement;
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that QuoVadis revoke the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is

any actual or suspected misuse or compromise of the Certificate Holder's Private Key associated with the Public Key listed in the Certificate; and

- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate.

Without limiting other Certificate Holder obligations stated in this CP/CPS, Certificate Holders are solely liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a Certificate the Certificate Holder represents to QuoVadis and to Relying Parties that at the time of acceptance and until further notice:

- The Certificate Holder retains control of the Certificate Holder's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorised use and that no unauthorised person has ever had access to the Certificate Holder's private key.
- All representations made by the Certificate Holder to QuoVadis regarding the information contained in the Certificate are accurate and true to the best of the Certificate Holder's knowledge or to the extent that the Certificate Holder receives notice of such information, the Certificate Holder shall act promptly to notify QuoVadis of any material inaccuracies contained in the Certificate.
- The Certificate is used exclusively for authorised and legal purposes, consistent with this CP/CPS, and that the Certificate Holder will use the Certificate only in conjunction with the entity named in the organisation field of the Certificate.
- The Certificate Holder agrees with the terms and conditions of this CP/CPS and other agreements and policy statements of QuoVadis.

9.6.4 Relying Parties Representations And Warranties

The Relying Party is solely responsible for making the decision to rely on a QuoVadis Certificate. A Relying Party accepts that in order to reasonably rely on a QuoVadis Certificate, the Relying Party must:

- Read and agree with the terms of the QuoVadis Relying Party Agreement including the limitations on the usage of the Certificate and also the limitations of liability for reliance on a QuoVadis Certificate.
- Verify the QuoVadis Certificate by referring to the relevant CRL in the QuoVadis Repository and trust the Certificate only if it is valid and has not been revoked or has expired.
- Rely on a QuoVadis Certificate only as may be reasonable under the circumstances, given (i) the Relying Party's previous course of dealing with the

Certificate Holder, (ii) the economic value of the transaction or communication, (iii) the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the transaction or communication, (iv) all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CP/CPS, and (v) any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Certificate Holder and/or the communication or transaction.

9.6.5 Representations And Warranties Of Other Participants

Not applicable.

9.7 Disclaimers Of Warranties

QuoVadis disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law. In no event and under no circumstances (except for fraud or wilful misconduct) shall QuoVadis be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages;
- Any costs, expenses, or loss of profits;
- Any death or personal injury;
- Any loss of data;
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates or digital signatures;
- Any other transactions or services offered within the framework of this CP/CPS;
- Any other damages except for those due to reliance, on the information featured on a Certificate, or on the verified information in a Certificate;
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or wilful misconduct of the Applicant or Certificate Holder;
- Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this CP/CPS;
- Any liability that arises from the usage of a Certificate that is not valid;
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CP/CPS;

- Any liability that arises from security, usability, integrity of products, including hardware and software a Certificate Holder uses; or
- Any liability that arises from compromise of a Certificate Holder's private key.

9.8 QuoVadis Liability

QuoVadis shall be liable to Certificate Holders or Relying Parties for direct loss arising from any breach of this CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to $5000 per Certificate Holder or Relying Party per Certificate. QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this Certificate Policy & Certification Practice Statement, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

9.8.1 Limitations of Liability

QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis' liability to any person for damages arising under, out of or related in any way to this CP/CPS, Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. QuoVadis shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the QuoVadis PKI (including, without limitation, the use of or reliance upon Certificates), any person that participates within the QuoVadis PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon

the foregoing as a condition and inducement to permit that person to participate within the QuoVadis Public Key Infrastructure.

9.8.2 Exclusions of Liability

QuoVadis shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorised disclosure or unauthorised use of the Certificate or any password or activation data used to control access thereto;
- If the Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or organisation;
- If the Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this QuoVadis CP/CPS and/or the relevant Certificate Holder Agreement or any applicable law or regulation;
- If the private key associated with the Certificate held by the claiming party or otherwise the subject of any claim has been compromised;
- If the Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that QuoVadis uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided QuoVadis uses commercially reasonable methods to protect against such disturbances;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of QuoVadis and/or its subcontractors or service providers; or
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil

disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which QuoVadis is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of QuoVadis.

9.8.3 Certificate Loss Limits

Without prejudice to any other provision of this Section 9, QuoVadis' liability for breach of its obligations pursuant to this QuoVadis CP/CPS shall, absent fraud or wilful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below.

Loss Limits/ Reliance Limits	Maximum per Certificate
Standard Certificates	US $250,000
Device Certificate	US $250,000

In no event shall QuoVadis' liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular Digital Certificate to the intent that the loss limits reflect QuoVadis' total potential cumulative liability per Digital Certificate per year (irrespective of the number of claims per Digital Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Digital Certificate in any one year of that Digital Certificate's life cycle.

9.9 Indemnities

Notwithstanding any limitations on its liability to Certificate Holders and Relying Parties, QuoVadis acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with QuoVadis do not assume any obligation or potential liability of QuoVadis under this CP/CPs or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. QuoVadis shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by QuoVadis, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by QuoVadis where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a

Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from QuoVadis online, and the application software either failed to check such status or ignored an indication of revoked status).

Any user of a QuoVadis Certificate, whether a Certificate Holder, Relying Party or otherwise, shall indemnify and hold harmless QuoVadis from any and all damages and losses arising out of: (i) use of the QuoVadis Certificate in a manner not authorised by QuoVadis; (ii) tampering with the QuoVadis Certificate; or (iii) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional. In addition, Certificate Holders shall indemnify and hold harmless QuoVadis from any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a QuoVadis Certificate relating to: (i) Certificate Holder's breach of its obligations under the Certificate Holder Agreement or this CP/CPS; (ii) Certificate Holder's failure to protect its private key; or (iii) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by Certificate Holder.

9.10 Term And Termination

9.10.1 Term

This CP/CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CP/CPS shall remain in force until it is amended or replaced by a new version in accordance with this Section 9.10.

9.10.3 Effect Of Termination And Survival

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

9.11 Individual Notices And Communications With Participants

Electronic mail, postal mail, fax, and web pages will all be valid means of QuoVadis providing any of the notices required by this CP/CPS, unless specifically provided

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

9.12 Amendments

9.12.1 Procedure For Amendment

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

9.12.2 Notification Mechanism And Period

The QuoVadis PMA reserves the right to amend this CP/CPS without notification for amendments that are not material, including typographical corrections, changes to URLs, and changes to contact details. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the QuoVadis PMA.

9.12.3 Circumstances Under Which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

Complaints can be communicated to QuoVadis via the QuoVadis website using the "Contact Us" link at https://www.quovadisglobal.com/ContactUs.aspx. Complaints can also be communicated to QuoVadis verbally by phoning the relevant QuoVadis office. A list of QuoVadis offices and contact details are provided at https://www.quovadisglobal.com/Locations.aspx. Complaints will be considered by QuoVadis management and then the appropriate steps will be taken.

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a "participant" within the QuoVadis PKI) arising out of or relating to this QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

9.14 Governing Law

This CP/CPS and any QuoVadis Certificates issued by QuoVadis are governed by the laws of the country referred to in the Certificate Holder Agreement for the Certificate in question, without reference to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods. Venue with respect to any dispute, controversy, or claim shall under the laws of the country referred to in the Certificate Holder Agreement for the Certificate in question.

9.15 Compliance With Applicable Law

Certificate Holders and Relying Parties shall use QuoVadis Certificates and any other related information and materials provided by QuoVadis only in compliance with all applicable laws and regulations. QuoVadis may refuse to issue or may revoke Certificates if, in the reasonable opinion of QuoVadis, issuance or the continued use of the QuoVadis Certificates would violate applicable laws or regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not Applicable.

9.16.2 Assignment

Parties to this CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of QuoVadis, and any such attempted assignment shall be void.

9.16.3 Severability

Any provision of this QuoVadis CP/CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this QuoVadis CP/CPS or affecting the validity or enforceability of such remaining provisions.

9.16.4 Enforcement (Waiver Of Rights)

Except where an express time frame is set forth in this CP/CPS, no delay or omission by QuoVadis to exercise any right, remedy, or power it has under this CP/CPS shall impair or be construed as a waiver of such right, remedy, or power. A waiver by QuoVadis of any breach or covenant in this CP/CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. No waiver shall be effective unless it is in writing. Bilateral agreements between QuoVadis and the parties to this CP/CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

QUOVADIS ACCEPTS NO LIABILITY FOR ANY BREACH OF WARRANTY, DELAY, OR FAILURE IN PERFORMANCE THAT RESULTS FROM EVENTS BEYOND ITS CONTROL SUCH AS ACTS OF GOD, ACTS OF WAR, ACTS OF TERRORISM, EPIDEMICS, POWER OR TELECOMMUNICATION SERVICES FAILURE, FIRE, AND OTHER NATURAL DISASTERS.

9.17 Other Provisions

No stipulation.

10 APPENDIX A – CA Profiles

QuoVadis Root CA2

Field	Value
Version	V3
Serial Number	Unique number 0509
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	25 years expressed in UTC format NotBefore: 11/24/2006 18:27:00 NotAfter: 11/24/2031 18:23:33
Subject Distinguished Name	CN = QuoVadis Root CA 2 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	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; KeyID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b Certificate Issuer: Directory Address: CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM Certificate SerialNumber=05 09
Subject Key Identifier	c=no; 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Key Usage	c=no; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=None
Key Id Hash(sha1):	73 97 82 ea b4 04 16 6e 25 d4 82 3c 37 db f8 a8 12 fb cf 26
Cert Hash(sha1):	ca 3a fb cf 12 40 36 4b 44 b2 16 20 88 80 48 39 19 93 7c f7

QuoVadis Root CA 2 G3

Field	Value
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 }
Extension	**Value**
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

QuoVadis Enterprise Trust CA 2 G3

Field	Value
Version	V3
Serial Number	Unique number 5eeeb44a70e18e63c9898f202cbac164914edc05
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 Root CA 2 G3 C=BM
Validity Period	10 years NotBefore: 6/6/2016 NotAfter: 6/6/2031
Subject Distinguished Name	CN=QuoVadis Enterprise Trust CA 2 G3 O=QuoVadis Limited C=BM
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d
Subject Key Identifier	c=no; KeyID= 64 e3 05 8b 26 be f3 35 f5 9f 31 12 08 f8 e4 16 9c 2a a8 62
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=none
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/qvrca2g3.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2g3.crl
Key Id Hash(sha256)	bdf1a27972ce71cbb7e898610463f5c9a154c317f766cf7f043d3540a4128b51
Cert Hash(sha256):	174e1de77c8d93c68ecd2bd2ea6e191b584db850277a834aac898b7c80a91c70

QuoVadis Global SSL ICA G2

Field	Value
Version	V3
Serial Number	Unique number 48982de2a92cb339e1c8f933358275d3e4f88255
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 6/1/2013 13:35 NotAfter: 6/1/2023 13:35
Subject Distinguished Name	CN = QuoVadis Global SSL ICA G2 O = QuoVadis Limited C = BM
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Subject Key Identifier	c=no; 91 19 62 ad 5b 17 a7 30 fb f0 de 39 25 b1 bd 8c b9 b8 51 27
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	c=no; Certificate Policies; {All issuance policies }
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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/qvrca2.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Key Id Hash(sha1):	98 58 bb 24 0e e4 4c 25 78 ac f3 9b 86 08 d1 5f 97 89 d9 7f
Cert Hash(sha1):	60 36 33 0e 16 43 a0 ce e1 9c 8a f7 80 e0 f3 e8 f5 9c a1 a3

QuoVadis Global SSL ICA G3

Field	Value
Version	V3
Serial Number	Unique number 7ed6e79cc9ad81c4c8193ef95d4428770e341317
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 G3 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 11/6/2012 14:50:18 NotAfter: 11/6/2022 14:50:18
Subject Distinguished Name	CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d
Subject Key Identifier	c=no; b3 12 89 b5 a9 4b 35 bc 15 00 f0 80 e9 d8 78 87 f1 13 7c 76
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	c=no; Certificate Policies; {All issuance policies }
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=1
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL = http://ocsp.quovadisglobal.com
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2g3.crl
Key Id Hash(sha1):	9a e2 98 4b 15 27 e9 9c f7 71 45 2b 27 d1 0e 5e dc 36 d5 41
Cert Hash(sha1):	e9 0b cc a3 d1 34 12 7e f6 46 e8 54 72 3f 13 7d 79 71 db 64

QuoVadis EV SSL ICA G1

Field	Value
Version	V3
Serial Number	Unique number 73da5afa23d93fba842e0a20f401c9d86e24fc5d
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years expressed in UTC format NotBefore: 13/1/2015 14:42:15 NotAfter: 13/1/2025 14:42:15
Subject Distinguished Name	CN = QuoVadis EV SSL ICA G1 O = QuoVadis Limited C = BM
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Subject Key Identifier	c=no; KeyID= 55 58 86 ce ba 7c 76 4e 99 13 a9 0f d3 6c 9f c2 f5 d3 3c e3
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Enhanced Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	c=no; [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.2
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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/qvrca2.crt

CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Key Id Hash(sha1):	d8 44 ec ec e9 e1 42 f6 9e f5 2b 53 ee 8f 11 e8 55 62 bf eb
Cert Hash(sha1):	62 85 32 b7 3d bb 41 a5 86 2a e4 af f7 49 e6 7a cb cb b5 60

QuoVadis EV SSL ICA G3

Field	Value
Version	V3
Serial Number	Unique number 524fc1f16e34d1702b84a13fb042bbcc7c3c9032
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 G3 O =QuoVadis Limited C = BM
Validity Period	10 years NotBefore: 30/11/2016 NotAfter: 30/11/2026
Subject Distinguished Name	CN = QuoVadis EV SSL ICA G3 O = QuoVadis Limited C = BM
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID=ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d
Subject Key Identifier	c=no; KeyID= e5 84 54 d0 90 49 9f 38 ba f2 c9 e1 2a 08 c5 4e 9f a0 48 3f
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Enhanced Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.2 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS

	Qualifier: http://www.quovadisglobal.com/repository
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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://crl.quovadisglobal.com/qvrca2g3.crl
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Key Id Hash(sha256):	c017a409cbf588b46160cb0816a11dbf354e14ed037a11afe5ec479a893ff13b
Cert Hash(sha256):	f18442bedf70b4d15211356c72b659332bed03ffd3bba7afaaabe6de9d723002

QuoVadis Code Signing CA G1

Field	Value
Version	V3
Serial Number	Unique number 1ce6507ec1d9c0b16178feee058cae7a0b142858
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years NotBefore: 5/30/2014 14:02 NotAfter: 5/30/2024 14:02
Subject Distinguished Name	CN = QuoVadis Code Signing CA G1 O = QuoVadis Limited C = BM
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Subject Key Identifier	c=no; 9d c1 5a 6b 5c a3 f1 29 c8 7d 48 b5 60 69 d7 a7 23 cd ee c9

Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	c=no; Certificate Policies; {All issuance policies}
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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://crl.quovadisglobal.com/qvrca2.crl
Enhanced Key Usage	c = no; Enhanced Key Usage= Code Signing (1.3.6.1.5.5.7.3.3)
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Key Id Hash(sha1):	15 20 b8 fa 81 19 22 85 81 bb fb 2c 94 33 36 f9 08 76 43 b1
Cert Hash(sha1):	af 27 a6 ef 0b 4c 8e 37 af a8 20 3e c9 40 ab f9 95 6d f0 57

QuoVadis Qualified Web ICA G1

Field	Value
Version	V3
Serial Number	Unique number 4984b32ba495d0c61de34bcf14d3a35aee508644
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Enterprise Trust CA 2 G3 O =QuoVadis Limited C = BM
Validity Period	10 years NotBefore: 16/3/2017 NotAfter: 14/3/2027
Subject Distinguished Name	CN = QuoVadis Qualified Web ICA G1 O = QuoVadis Trustlink B.V. OID.2.5.4.97=NTRNL-30237459 C = NL
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID=64 e3 05 8b 26 be f3 35 f5 9f 31 12 08 f8 e4 16 9c 2a a8 62

Subject Key Identifier	c=no; KeyID= 04 bb 04 d7 9d d8 7d 1c d9 e4 f0 54 bd 8c 3c b6 32 de 76 34
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Enhanced Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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://crl.quovadisglobal.com/qvrca2g3.crl
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Key Id Hash(sha256):	0177577710eab1bf1df1e4ac44f63961c9d16390bdd8d1f815d8ae7230fbcf1b
Cert Hash(sha256):	c02d8a30ed69b2f864ed8fb1a63a3e7255288920ca294bdca30f63898fb9195c

HydrantID EV SSL ICA G1

Field	Value
Version	V3
Serial Number	Unique number 5bfdd1bb152d106baa6d6d17e73c561f0dd9c8ca
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM

Validity Period	10 years NotBefore: 13/1/2015 NotAfter: 13/1/2025
Subject Distinguished Name	CN = HydrantID EV SSL ICA G1 O = HydrantID (Avalanche Cloud Corporation) C = US
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= 1a8462bc484c332504d4eed0f603c41946d1946b
Subject Key Identifier	c=no; KeyID= 54753e33d17d142e4b7009c4ac5d4ad1833978b5
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.2 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.3.900.0 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.hydrantid.com/support/repository
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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/qvrca2.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Cert Hash(sha256):	80FDE428212AF0CA0AC531EEE6ED2DF3D3C2A4557DFCE857070FC947922E9B24

HydrantID SSL ICA G2

Field	Value
Version	V3
Serial Number	Unique number 7517167783d0437eb556c357946e4563b8ebd3ac
Issuer Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	10 years NotBefore: 17/12/2013 NotAfter: 17/12/2023
Subject Distinguished Name	CN = HydrantID EV SSL ICA G2 O = HydrantID (Avalanche Cloud Corporation) C = US
Subject Public Key Information	4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	sha256RSA {1.2.840.113549.1.1.11 }
Extension	**Value**
Authority Key Identifier	c=no; KeyID= 1a8462bc484c332504d4eed0f603c41946d1946b
Subject Key Identifier	c=no; KeyID= 986ab62d2ebfa7aa9ff6f7d609afd58b57f98ab7
Key Usage	c=yes; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.2.100.1.2 [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.3.900.0 [4,1]Policy Qualifier Info:

	Policy Qualifier Id=CPS Qualifier: http://www.hydrantid.com/support/repository
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=0
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/qvrca2.crt
CRL Distribution Points	c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvrca2.crl
Cert Hash(sha256):	9C6D08933201407FBF2B12540B67CC0E4C9666F132E1504762A717CBAE8F3FD6

11 APPENDIX B

11.1 Business SSL

Field	Value
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	Unique X.500 CA DN. CN = QuoVadis Global SSL ICA or CN = QuoVadis Global SSL ICA G2 or CN = QuoVadis Global SSL ICA G3 or CN = QuoVadis Europe SSL CA G1 or CN = QuoVadis Grid ICA G2 O = QuoVadis Limited C = BM
Validity Period	1, 2, or 3 years expressed in UTC format
Subject Distinguished Name	
Organization Name	subject:organisationName (2.5.4.10)
Organisation Unit	subject:organisationUnit (2.5.6.5) Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)
Country	subject:countryName (2.5.4.6)
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)
Extension	**Value**
Authority Key Identifier	c=no; Octet String – Same as Issuer's Subject Key Identifier
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)

Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository
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/<CA Name>.crl

Purposes of Business SSL

Purposes of Business SSL

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

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

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

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

Eligible Applicants

Individuals (natural persons), incorporated entities, government entities, general partnerships, unincorporated associations, and sole proprietorships may apply for QuoVadis Business SSL Certificates.

Verification Requirements

Before issuing a Business SSL Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and has accepted a Certificate Holder Agreement for the requested Certificate.

Identity: QuoVadis verifies the identity and address of the organization and that the address is the Applicant's address of existence or operation. QuoVadis verifies the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

DBA/Tradename: If the Subject Identity Information is to include a DBA or tradename, QuoVadis verifies the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

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

a) 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;
b) the ccTLD of the requested Domain Name;
c) information provided by the Domain Name Registrar; or
d) 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 Certificate Holder Agreement and approves Certificate issuance. Step 4: All signatures are verified through follow-up procedures or telephone calls.

Step 5: QuoVadis obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the Certificate Request and notify the Applicant accordingly. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 6: QuoVadis creates the Business SSL Certificate.

Step 7: The Business SSL Certificate is delivered to the Applicant.

Renewal

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

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 = QuoVadis EV SSL ICA G1 or CN = QuoVadis Global SSL ICA G2 or CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	
Validity Period	1 or 2 years expressed in UTC format	
Subject Distinguished Name		
Organization Name	subject:organisationName (2.5.4.10)	This field MUST contain the Subject's full legal organisation name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organisation name in parenthesis. If the combination of the full legal organisation name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organisation name will be used.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard Certificates are not allowed for EV Certificates.

City or Town of Incorporation	subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows.
State/Province of Incorporation	subject:jurisdictionOfIncorporationStateOrProvin ceName (1.3.6.1.4.1.311.60.2.1.2)	ASN.1 - X520StateOrProvinceName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above.
Country of Incorporation	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)	ASN.1 - X520countryName as specified in RFC 5280 Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code.
Registration Number	Subject:serialNumber (2.5.4.5)	For Private Organisations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number or verifiable date of creation, the field will contain the label “Government Entity”.
Business Category	Subject:businessCategory (2.5.4.15)	This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject.
Number & street (optional)	subject:streetAddress (2.5.4.9)	
City or town	subject:localityName (2.5.4.7)	

State or province (if any)	subject:stateOrProvinceName (2.5.4.8)
Country	subject:countryName (2.5.4.6)
Postal code (optional)	subject:postalCode (2.5.4.17)
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)

Extension	Value
Authority Key Identifier	c=no; Octet String – Same as Issuer's Subject Key Identifier
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.2 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 2 Certification Policies and Certificate Practice Statement.
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

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;
- Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number; and
- Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

EV SSL also help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence; provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud; and assist law enforcement in investigations including where appropriate, contacting, investigating, or taking legal action against the Subject.

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

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

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:

a) 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.

b) 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.

c) 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 Certificate Holder 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.

d) Non-Commercial Entity Subjects

Non-Commercial Entities are entities who do not qualify under subsections (a), (b) or (c) above, but that do satisfy the following requirements:

- The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of International Organizations that have been approved for EV eligibility; and
- The International Organization Entity MUST NOT be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
- The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Subsidiary organizations or agencies of qualified International Organizations may also qualify for EV Certificates issued in accordance with the EV Guidelines.

Additional Warranties and Representations for EV Certificates

QuoVadis makes the following EV Certificate Warranties solely to Certificate Holders, Certificate Subjects, Application Software Suppliers with whom QuoVadis has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Suppliers, and all Relying Parties that actually rely on such EV Certificate during the period when it is valid, that it followed the requirements of the EV

Guidelines and this CP/CPS in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (EV Certificate Warranties).

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

- Legal Existence: QuoVadis has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organisation or entity in the Jurisdiction of Incorporation or Registration;
- Identity: QuoVadis has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: QuoVadis has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;
- Authorization for EV Certificate: QuoVadis has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorised the issuance of the EV Certificate;
- Accuracy of Information: QuoVadis has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- Certificate Holder Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Certificate Holder 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
- Revocation: QuoVadis will follow the requirements of the EV Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in the EV Guidelines.

Verification Requirements

Before issuing an EV Certificate, QuoVadis ensures that all Subject organisation information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and

documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

I. Verify Applicant's existence and identity, including;

- Verify Applicant's legal existence and identity (as established with an Incorporating Agency),
- Verify Applicant's physical existence (business presence at a physical address), and
- Verify Applicant's operational existence (business activity).

II. Verify Applicant (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV Certificate;

III. Verify Applicant's authorization for the EV Certificate, including;

- Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
- Verify that Contract Signer signed the Certificate Holder Agreement; and
- Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

The vetting regime of the EV Guidelines includes detailed verification procedures, which vary by Certificate Holder, and may include direct confirmation with Incorporating Agencies as well as correlation of information from certain qualified commercial data providers, site visits, and independent confirmations from senior officers of the Applicant. Verified opinion letters from attorneys and accountants representing the Applicant, as well as bank account verifications, may also be used to fulfil aspects of the vetting process.

Applicant Contacts

The EV Guidelines specify a number of Applicant roles involved in the EV verification process. All must be filled by natural persons (i.e., specific individuals as opposed to generic titles or automated systems). The Applicant may authorize one individual to occupy two or more of these roles. The Applicant may authorize more than one individual to occupy any of these roles.

QuoVadis requires Applicants for EV Certificates to execute an EV Authority Letter to identify and authorise the various Applicant contacts, as well as to enable the use of online confirmations and approvals for various aspects of the EV process.

- Certificate Requester: The initial contact that submits the Certificate Application to QV on behalf of the Applicant. This person does NOT need to be an employee of the Applicant, but must be an authorised agent with express authority to

represent the Applicant. Certificate Requesters are formally recognised by QuoVadis only after QuoVadis has confirmed their appointment with the Applicant.

- Certificate Approver: MUST be either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
- Contract Signer: MUST be either the Applicant, employed by the Applicant, or an authorized 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.

Certificate Holder Agreement

Each Applicant must enter into a Certificate Holder 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:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the QuoVadis, both in the EV Certificate Request and as otherwise requested by the QuoVadis in connection with the issuance of the EV Certificate(s) to be supplied by the QuoVadis;
- Protection of Private Key: An obligation and warranty by the Certificate Holder or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device – e.g., password or token);
- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at a domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorised company business, and solely in accordance with the Certificate Holder Agreement;

- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request the QuoVadis to revoke the EV Certificate, in the event that:

  (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Certificate Holder's Private Key associated with the Public Key listed in the EV Certificate; and
- Termination of Use of EV Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

Application Process

During the Certificate approval process, QuoVadis Validation Specialists employ controls to validate the identity of the Certificate Holder and other information featured in the Certificate Application to ensure compliance with the Guidelines.

Step 1: The Certificate Requester provides a signed Certificate Application to QuoVadis, which includes information about the Applicant, personnel within the organisation who have authority to approve the request and also agreement to the Certificate Holder Agreement. In addition, the Certificate Requester provides a PKCS#10 CSR as well as billing information for processing the request and issuing the EV Certificate.

Step 2: QuoVadis independently verifies all information that is required to be verified by the EV Guidelines using a variety of sources.

Step 3: QuoVadis requests and receives a signed EV Authority Letter from the Applicant (unless a valid EV Authority Letter from the Applicant is already in its possession). Alternate procedures may also be used to authenticate the identity and authority of individuals involved in the Certificate Application.

Step 4: The Certificate Approver is contacted to obtain approval of Certificate issuance.

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 by the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the EV Certificate Request and notify the Applicant accordingly.

Renewal

Under the EV Guidelines, renewal requirements and procedures are generally the same as those employed for the validation and issuance for new Applicants. The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is thirteen months, except for the identity and authority of individuals identified in the EV Authority Letter.

In the case of outdated information, QuoVadis repeats the verification processes required by the EV Guidelines. If a company is no longer in good standing, or if any of the other required information cannot be verified, the Certificate is not renewed.

11.3 QuoVadis Qualified Website Authentication (QCP-w)

ETSI EN 319 411-2 defines “QCP-w“ as the “policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person”.

QuoVadis policy is that QuoVadis Qualified Website Authentication (QCP-w) certificates (also known as QWAC) will only be issued to legal persons and not natural persons.

QuoVadis QCP-w certificates will be 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]. In addition, EU qualified certificates issued under this policy may be used to 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 certificate profile below is designed in accordance with:

- The EV Guidelines;
- ETSI EN 319 411-2;
- ETSI EN 319 412-4; and
- ETSI EN 319 412-5:

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 = QuoVadis Qualified Web ICA G1 O = QuoVadis Trustlink B.V. Org Id = NTRNL-30237459 C = NL	
Validity Period	1 or 2 years expressed in UTC format	

Subject Distinguished Name		
Organization Name	subject:organisationName (2.5.4.10)	This field MUST contain the Subject's full legal organisation name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organisation name in parenthesis. If the combination of the full legal organisation name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organisation name will be used.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard Certificates are not allowed for EV Certificates.
City or Town of Incorporation	subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	ASN.1 - X520LocalityName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows.
State/ Province of Incorporation	subject:jurisdictionOfIncorporationStateOrProvin ceName (1.3.6.1.4.1.311.60.2.1.2)	ASN.1 - X520StateOrProvinceName as specified in RFC 5280 Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above.
Country of Incorporation	subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)	ASN.1 - X520countryName as specified in RFC 5280 Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country

		information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code.
Registration Number	Subject:serialNumber (2.5.4.5)	For Private Organisations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number or verifiable date of creation, the field will contain the label “Government Entity”.
Business Category	Subject:businessCategory (2.5.4.15)	This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject.
City or town	subject:localityName (2.5.4.7)	City or town
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	State or province (if any)
Country	subject:countryName (2.5.4.6)	Country
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	Subject Public Key Information
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	Signature Algorithm
Extension	**Value**	
Authority Key Identifier	c=no; Octet String – Same as Issuer's Subject Key Identifier	
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)	
Extended Key Usage	c=no;	

	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Certificate Policies	c=no; [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.quovadisglobal.com/repository [4] Certificate Policy: Policy Identifier=2.23.140.1.1	[1] QCP-W policy from ETSI EN 319 411-2 [2] QuoVadis EV policy OID [3] QuoVadis Qualified (not on QSCD policy OID [4] CAB Forum EV OID
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 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	
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
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
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) certificate are consistent with the vetting requirements for a QuoVadis EV SSL certificate, with the additional verification:

QuoVadis policy is that QuoVadis Qualified Website Authentication (QCP-w) certificates are only issued to legal persons and not natural persons. The identity of the legal person and, if applicable, any specific attributes of the legal person, shall be verified:

I. by the physical presence of an authorized representative of the legal person; or
II. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which QuoVadis can prove the equivalence.

11.4 Code Signing

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		
Organization Name	subject:organisationName (2.5.4.10)	Required field. The Subject's verified legal name.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Optional field. Must not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless QuoVadis has verified this information
Common Name	subject:commonName (2.5.4.3)	Required field. The Subject's verified legal name.
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	Required if the subject:localityName field is absent. Optional if the subject:localityName fields is present.
Locality	subject:locality (2.5.4.6)	Required if the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field is present.
Country	subject:countryName (2.5.4.6)	Required field.
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	
Extension	**Value**	

Authority Key Identifier	c=no; Octet String	
Subject Key Identifier	c=no; Octet String	
Key Usage	c=yes; Digital Signature (80)	
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codeSigning)	
Field	**Value**	**Comments**
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; { 2.23.140.1.4.1 } [1,1] Policy Qualifier Info: Policy Identifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository	1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID. 2.23.140.1.4.1 is the Code Signing Minimum Requirements OID.
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 - id-ad-caIssuers (Certification Authority Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/qvcscag1.crt	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/qvcscag1.crl	

Purposes of Code Signing

The primary purpose of QuoVadis Code Signing Certificates is to establish that executable code originates from a source identified by QuoVadis. QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended to provide any assurances, or otherwise represent or warrant:

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

Eligible Applicants

QuoVadis only issues Code Signing Certificates to Organisational Applicants and does not issue such certificates to Individual Applicants..

An Individual Applicant is an Applicant that is an individual and requests a Certificate that will list the Applicant's legal name as the Certificate subject.

An Organisational Applicant is an Applicant that requests a Certificate subject other than the name of an individual. Organisational Applicants include private and public corporations, LLCs, partnerships, government entities, non-profit organizations, trade associations, and other entities.

Private Key Protection

Certificate Holder Key Pairs must be generated and protected in one of the following options:

- A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Certificate Holder's private key protection through a TPM key attestation
- 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 Certificate Holder 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:

1. Verifies the Applicant's possession of the Private Key;
2. Verifies the Subject's legal identity, including any Doing Business As (DBA) as described in section 3.2.2.2 of the Baseline Requirements,
3. Verifies the Subject's address, and
4. Verifies the Certificate Requester's authority to request a certificate and the authenticity of the Certificate request using a verified method of communication.

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

1. the identity of the person performing the verification,

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

Application Process

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

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

Step 2: QuoVadis independently verifies information using a variety of sources in accordance with the “Verification Requirements” section above.

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

Step 5: QuoVadis obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the Certificate Request and notify the Applicant accordingly. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 6: QuoVadis creates the Code Signing Certificate.

Step 7: The Certificate is delivered to the Applicant.