# DigiCert Europe / QuoVadis

# Certification Policy/ Certification Practice Statement

Effective Date: 22 November, 2023

Version: 5.0

**Important Note About this Document**

This document is the Certificate Policy/Certification Practice Statement (CP/CPS) of DigiCert Europe (also known as QuoVadis), a company of DigiCert, Inc.

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.

This document covers aspects of the QuoVadis PKI. Services for PKIoverheid operate under a separate CP/CPS document.

There are a number of instances where the legal and regulatory frameworks for Qualified Certificates under the Swiss or EU Digital Signature regimes impose additional requirements. In these instances, this Document shows these differences either by indicating in the body of the text "For Qualified Certificates" or with the inclusion of a Text Box as shown below.

| | |
|---|---|
| | Provision relating to Qualified or Regulated Certificates issued in accordance with Swiss regulations. |
| | Provision relating to Qualified Certificates issued in accordance with Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation). |

**Contact Information**

- **Bermuda**: DigiCert Bermuda Limited (previously QuoVadis Limited), Washington Mall 3F, 7 Reid Street, Hamilton HM-11, Bermuda. Phone: +1-441-278-2800
- **Belgium:** DigiCert Europe Belgium BV (previously QuoVadis Trustlink BVBA), Schaliënhoevedreef 20T, 2800 Mechelen, Belgium. Phone: +32 15-79-65-21
- **Germany: DigiCert Deutschland GmbH** (previously QuoVadis Trustlink Deutschland GmbH), Ismaninger Str. 52, D-81675 München, Germany. Phone: +49-89-540-42-45-42
- **Ireland:** DigiCert Ireland Limited, 3 Dublin Landings, North Wall Quay, Dublin 1, D01C4EO, Ireland. Phone +353 1803 5400.
- **Netherlands:** QuoVadis Trustlink BV, Nevelgaarde 56 noord, 3436 ZZ Nieuwegein, Netherlands. Phone: +31 (0) 30 232-4320
- **Switzerland:** QuoVadis Trustlink Schweiz AG, Poststrasse 17, Postfach, 9001 St. Gallen, Switzerland. Phone: +41 71-228-98-00
- **United Kingdom:** QuoVadis Online Limited, 2 Harbour Exchange Square, London, E14 9GE, United Kingdom. Phone: +44 (0) 333-666-2000

Website: https://www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com
Problem reporting: https://www.quovadisglobal.com/certificate-revocation
Customer complaints: qvcomplaints@digicert.com

**Version Control**

| Author | Date | Version | Comment |
|---|---|---|---|
| QuoVadis PMA | 22 November, 2023 | 5.00 | Consolidation of previous CP/CPS documents (CP/CPS for Root CA and Root CA3 v4.43 and CP/CPS for Root CA2 v2.21) into a combined document. Prior version changes are tracked in those previous documents.<br>Transition to EU Cert Central, with minor editorial updates. Deprecation of HydrantID OID. Updates to Section 1.6.3 References, 4.12 escrow, 5.5 records archival, 6.3.1 public key archival, 6.5.1 and 6.5.2 computer security, 7.1.2 extensions, and Appendix A Standard profile OID options. |

**TABLE OF CONTENTS**


1. INTRODUCTION ..... 1
   - 1.1. Overview ..... 1
   - 1.2. Document Name And Identification ..... 1
   - 1.3. Public Key Infrastructure Participants ..... 2
     - 1.3.1. Certification Authorities ..... 2
     - 1.3.2. Registration Authorities and Other Delegated Third Parties ..... 2
     - 1.3.3. Subscribers ..... 3
     - 1.3.4. Relying Parties ..... 3
     - 1.3.5. Other Participants ..... 3
   - 1.4. Certificate Usage ..... 3
     - 1.4.1. Appropriate Certificate Uses ..... 3
     - 1.4.2. Prohibited Certificate Usage ..... 3
   - 1.5. Policy Administration ..... 4
     - 1.5.1. Organisation Administering The CP/CPS ..... 4
     - 1.5.2. Contact Person ..... 4
     - 1.5.3. Person Determining The CP/CPS Suitability ..... 5
     - 1.5.4. CP/CPS Approval Procedures ..... 5
   - 1.6. Definitions and Acronyms ..... 5
     - 1.6.1. Definitions ..... 5
     - 1.6.2. Acronyms ..... 7
     - 1.6.3. References ..... 8
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES ..... 10
   - 2.1. Repositories ..... 10
   - 2.2. Publication of Certificate Information ..... 10
   - 2.3. Time or Frequency of Publication ..... 10
   - 2.4. Access Controls on Repositories ..... 11
3. IDENTIFICATION AND AUTHENTICATION ..... 11
   - 3.1. Naming ..... 11
     - 3.1.1. Types Of Names ..... 11
     - 3.1.2. Need For Names To Be Meaningful ..... 11
     - 3.1.3. Pseudonymous Subscribers ..... 11
     - 3.1.4. Rules For Interpreting Various Name Forms ..... 11
     - 3.1.5. Uniqueness Of Names ..... 12
     - 3.1.6. Recognition, Authentication, And Role Of Trademarks ..... 12
   - 3.2. Initial Identity Validation ..... 12
     - 3.2.1. Method To Prove Possession Of Private Key ..... 12
     - 3.2.2. Authentication Of Organisation Identity ..... 12
     - 3.2.3. Authentication Of Individual Identity ..... 15
     - 3.2.4. Non-Verified Subscriber Information ..... 18
     - 3.2.5. Validation Of Authority ..... 18
     - 3.2.6. Criteria for Interoperation ..... 18
   - 3.3. Identification And Authentication For Re-Key Requests ..... 18
     - 3.3.1. Identification And Authentication For Routine Re-Key ..... 18
     - 3.3.2. Identification and Authentication For Re-Key After Revocation ..... 19
   - 3.4. Identification and Authentication For Revocation Requests ..... 19
4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS ..... 19
   - 4.1. Certificate Application ..... 19
     - 4.1.1. Who Can Submit A Certificate Application ..... 19
     - 4.1.2. Enrolment Process And Responsibilities ..... 19
   - 4.2. Certificate Application Processing ..... 20
     - 4.2.1. Performing Identification And Authentication Functions ..... 20
     - 4.2.2. Approval Or Rejection Of Certificate Applications ..... 20
     - 4.2.3. Time To Process Certificate Applications ..... 21
   - 4.3. Certificate Issuance ..... 21

4.3.1. CA Actions During Certificate Issuance ..... 21
4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate ..... 21
4.3.3. Notification to NCA for PSD2 Certificates ..... 21
4.4. Certificate Acceptance ..... 21
4.4.1. Conduct Constituting Certificate Acceptance ..... 21
4.4.2. Publication Of The Certificate By The CA ..... 22
4.4.3. Notification Of Certificate Issuance By The CA To Other Entities ..... 22
4.5. Key Pair And Certificate Usage ..... 22
4.5.1. Subscriber Private Key And Certificate Usage ..... 22
4.5.2. Relying Party Public Key And Certificate Usage ..... 22
4.6. Certificate Renewal ..... 22
4.6.1. Circumstance For Certificate Renewal ..... 22
4.6.2. Who May Request Renewal ..... 23
4.6.3. Processing Certificate Renewal Requests ..... 23
4.6.4. Notification Of New Certificate Issuance To Subscriber ..... 23
4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate ..... 23
4.6.6. Publication of the Renewal Certificate By The CA ..... 23
4.6.7. Notification Of Certificate Issuance By The CA To Other Entities ..... 23
4.7. Certificate Re-Key ..... 23
4.7.1. Circumstance For Certificate Re-Key ..... 23
4.7.2. Who May Request Re-Key ..... 23
4.7.3. Processing Certificate Re-Key Request ..... 23
4.7.4. Notification Of Certificate Re-Key To Subscriber ..... 23
4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate ..... 24
4.7.6. Publication Of The Re-Key Certificate By The CA ..... 24
4.7.7. Notification Of Certificate Re-Key By The CA To Other Entities ..... 24
4.8. Certificate Modification ..... 24
4.8.1. Circumstances For Certificate Modification ..... 24
4.8.2. Who May Request Certificate Modification ..... 24
4.8.3. Processing Certificate Modification Requests ..... 24
4.8.4. Notification Of Certificate Modification To Subscriber ..... 24
4.8.5. Conduct Constituting Acceptance Of A Modified Certificate ..... 24
4.8.6. Publication Of The Modified Certificate By The CA ..... 24
4.8.7. Notification Of Certificate Modification By The CA To Other Entities ..... 24
4.9. Certificate Revocation And Suspension ..... 24
4.9.1. Circumstances For Revocation ..... 25
4.9.2. Who Can Request Revocation ..... 27
4.9.3. Procedure For Revocation Request ..... 27
4.9.4. Revocation Request Grace Period ..... 28
4.9.5. Time Within Which The CA Must Process The Revocation Request ..... 28
4.9.6. Revocation Checking Requirement For Relying Parties ..... 29
4.9.7. CRL Issuance Frequency ..... 29
4.9.8. Maximum Latency For CRL ..... 29
4.9.9. On-Line Revocation/Status Checking Availability ..... 29
4.9.10. OCSP Checking Requirement ..... 29
4.9.11. Other Forms Of Revocation Advertisements Available ..... 29
4.9.12. Special Requirements Related To Key Compromise ..... 30
4.9.13. Circumstances For Suspension ..... 30
4.9.14. Who Can Request Suspension ..... 30
4.9.15. Procedure For Suspension Request ..... 30
4.9.16. Limits On Suspension Period ..... 30
4.10. Certificate Status Services ..... 30
4.10.1. Operational Characteristics ..... 30
4.10.2. Service Availability ..... 31
4.10.3. Optional Features ..... 31
4.11. End Of Subscription ..... 31

4.12. Key Escrow And Recovery ..... 31
4.12.1. Key Escrow And Recovery Policy And Practices ..... 31
4.12.2. Session Key Encapsulation And Recovery Policy And Practices ..... 31
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ..... 32
5.1. Physical Controls ..... 32
5.1.1. Site Location and Construction ..... 32
5.1.2. Physical Access ..... 32
5.1.3. Power And Air-Conditioning ..... 32
5.1.4. Water Exposures ..... 32
5.1.5. Fire Prevention And Protection ..... 32
5.1.6. Media Storage ..... 32
5.1.7. Waste Disposal ..... 33
5.1.8. Off-Site Backup ..... 33
5.2. Procedural Controls ..... 33
5.2.1. Trusted Roles ..... 33
5.2.2. Number Of Persons Required Per Task ..... 34
5.2.3. Identification And Authentication For Each Role ..... 34
5.2.4. Roles Requiring Separation Of Duties ..... 34
5.3. Personnel Controls ..... 34
5.3.1. Qualifications, Experience, And Clearance Requirements ..... 34
5.3.2. Background Check Procedures ..... 34
5.3.3. Training Requirements ..... 35
5.3.4. Retraining Frequency And Requirements ..... 35
5.3.5. Job Rotation Frequency And Sequence ..... 35
5.3.6. Sanctions For Unauthorised Actions ..... 35
5.3.7. Independent Contractor Requirements ..... 35
5.3.8. Documentation Supplied To Personnel ..... 35
5.4. Audit Logging Procedures ..... 35
5.4.1. Types Of Events Recorded ..... 35
5.4.2. Frequency Of Processing Log ..... 36
5.4.3. Retention Period For Audit Log ..... 36
5.4.4. Protection Of Audit Log ..... 37
5.4.5. Audit Log Backup Procedures ..... 37
5.4.6. Audit Collection System ..... 37
5.4.7. Notification To Event-Causing Subject ..... 37
5.4.8. Vulnerability Assessment ..... 37
5.5. Records Archival ..... 37
5.5.1. Types Of Records Archived ..... 37
5.5.2. Retention Period For Archive ..... 38
5.5.3. Protection Of Archive ..... 38
5.5.4. Archive Backup Procedures ..... 39
5.5.5. Requirements For Time-Stamping Of Records ..... 39
5.5.6. Archive Collection System ..... 39
5.5.7. Procedures To Obtain And Verify Archive Information ..... 39
5.6. Key Changeover ..... 39
5.7. Compromise And Disaster Recovery ..... 39
5.7.1. Incident and Compromise Handling Procedures ..... 39
5.7.2. Computing Resources, Software, and/or Data Are Corrupted ..... 39
5.7.3. Entity Private Key Compromise Procedures ..... 39
5.7.4. Business Continuity Capabilities After a Disaster ..... 40
5.8. CA And/Or RA Termination ..... 40
6. TECHNICAL SECURITY CONTROLS ..... 41
6.1. Key Pair Generation And Installation ..... 41
6.1.1. Key Pair Generation ..... 41
6.1.2. Private Key Delivery To Subscriber ..... 41
6.1.3. Public Key Delivery To Certificate Issuer ..... 42

6.1.4. CA Public Key To Relying Parties ..... 42
6.1.5. Key Sizes ..... 42
6.1.6. Public Key Parameters Generation And Quality Checking ..... 43
6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field) ..... 43
6.2. Private Key Protection And Cryptographic Module Engineering Controls ..... 43
6.2.1. Cryptographic Module Standards And Controls ..... 43
6.2.2. Private Key (N of M) Multi-Person Control ..... 44
6.2.3. Private Key Escrow ..... 44
6.2.4. Private Key Backup ..... 44
6.2.5. Private Key Archive ..... 44
6.2.6. Private Key Transfer Into Or From A Cryptographic Module ..... 44
6.2.7. Private Key Storage On Cryptographic Module ..... 44
6.2.8. Method Of Activating Private Key ..... 45
6.2.9. Method Of Deactivating Private Key ..... 45
6.2.10. Method Of Destroying Private Key ..... 45
6.2.11. Cryptographic Module Rating ..... 45
6.3. Other Aspects Of Key Pair Management ..... 45
6.3.1. Public Key Archival ..... 45
6.3.2. Certificate Operational Periods And Key Pair Usage Periods ..... 45
6.4. Activation Data ..... 46
6.4.1. Activation Data Generation And Installation ..... 46
6.4.2. Activation Data Protection ..... 46
6.4.3. Other Aspects Of Activation Data ..... 46
6.5. Computer Security Controls ..... 46
6.5.1. Specific Computer Security Technical Requirements ..... 47
6.5.2. Computer Security Rating ..... 47
6.6. Life Cycle Technical Controls ..... 47
6.6.1. System Development Controls ..... 47
6.6.2. Security Management Controls ..... 48
6.6.3. Life Cycle Security Controls ..... 48
6.7. Network Security Controls ..... 48
6.8. Time-Stamping ..... 48
7. CERTIFICATE, CRL, AND OCSP PROFILES ..... 48
7.1. Certificate Profile ..... 49
7.1.1. Version Number(s) ..... 49
7.1.2. Certificate Extensions ..... 49
7.1.3. Algorithm Object Identifiers ..... 49
7.1.4. Name Forms ..... 50
7.1.5. Name Constraints ..... 50
7.1.6. CP/CPS Object Identifier ..... 51
7.1.7. Usage Of Policy Constraints Extension ..... 51
7.1.8. Policy Qualifiers Syntax And Semantics ..... 51
7.1.9. Processing Semantics For The Critical Certificate Policies Extension ..... 51
7.2. CRL Profile ..... 51
7.2.1. Version Number ..... 53
7.2.2. CRL And CRL Entry Extensions ..... 54
7.3. OCSP Profile ..... 54
7.3.1. OCSP Version Numbers ..... 54
7.3.2. OCSP Extensions ..... 54
7.4. Certificate Fields and Root CA Certificate Hashes ..... 55
*7.4.1.* Certificate Fields ..... 55
7.4.2. QuoVadis Root Certificate Hashes ..... 56
7.5. Certificate Transparency ..... 57
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS ..... 57
8.1. Frequency, Circumstance And Standards Of Assessment ..... 57
8.2. Identity And Qualifications Of Assessor ..... 57

8.3. Assessor's Relationship To Assessed Entity ..... 57
8.4. Topics Covered By Assessment ..... 57
8.5. Actions Taken As A Result Of Deficiency ..... 57
8.6. Communication Of Audit Results ..... 58
8.7. Self Audits ..... 58
9. OTHER BUSINESS AND LEGAL MATTERS ..... 58
9.1. Fees ..... 58
9.1.1. Certificate Issuance Or Renewal Fees ..... 58
9.1.2. Certificate Access Fees ..... 58
9.1.3. Revocation Or Status Information Access Fees ..... 58
9.1.4. Fees For Other Services ..... 58
9.1.5. Refund Policy ..... 58
9.2. Financial Responsibilities ..... 59
9.2.1. Insurance Coverage ..... 59
9.2.2. Other Assets ..... 59
9.2.3. Insurance Or Warranty Coverage For End-Entities ..... 59
9.2.4. Fiduciary Relationships ..... 59
9.3. Confidentiality Of Business Information ..... 59
9.3.1. Scope Of Confidential Information ..... 59
9.3.2. Information Not Within The Scope Of Confidential Information ..... 60
9.3.3. Responsibility To Protect Confidential Information ..... 60
9.4. Privacy Of Personal Information ..... 60
9.4.1. Privacy Plan ..... 60
9.4.2. Information Treated As Private ..... 60
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
9.4.7. Other Information Disclosure Circumstances ..... 61
9.5. Intellectual Property Rights ..... 61
9.5.1. Property Rights In Certificates And Revocation Information ..... 61
9.5.2. Property Rights In The CP/CPS ..... 61
9.5.3. Property Rights In Names ..... 61
9.5.4. Property Rights In Keys And Key Material ..... 61
9.5.5. Violation Of Property Rights ..... 61
9.6. Representations And Warranties ..... 61
9.6.1. CA Representations And Warranties ..... 61
9.6.2. RA Representations And Warranties ..... 62
9.6.3. Subscriber 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. Liability and Limitations of Liability ..... 64
9.9. Indemnities ..... 65
9.9.1. Indemnification By QuoVadis ..... 65
9.9.2. Indemnification By Subscribers ..... 65
9.9.3. Indemnification By Relying Parties ..... 65
9.10. Term And Termination ..... 66
9.10.1. Term ..... 66
9.10.2. Termination ..... 66
9.10.3. Effect Of Termination And Survival ..... 66
9.11. Individual Notices And Communications With Participants ..... 66
9.12. Amendments ..... 66
9.12.1. Procedure For Amendment ..... 66
9.12.2. Notification Mechanism And Period ..... 66
9.12.3. Circumstances Under Which Object Identifiers Must Be Changed ..... 66

9.13. Dispute Resolution Provisions ..... 66
9.14. Governing Law ..... 67
9.15. Compliance With Applicable Law ..... 68
9.16. Miscellaneous Provisions ..... 68
9.16.1. Entire Agreement ..... 68
9.16.2. Assignment ..... 69
9.16.3. Severability ..... 69
9.16.4. Enforcement (Attorneys' Fees And Waiver Of Rights) ..... 69
9.16.5. Force Majeure ..... 69
9.17. Other Provisions ..... 69
10. APPENDIX A ..... 70
10.1. Certificate Profiles ..... 70
10.1.1. QuoVadis Certificate Class ..... 70
10.1.2. Key Usage And Escrow ..... 72
10.2. QV Standard ..... 73
10.3. QV Advanced ..... 74
10.4. QV Advanced + ..... 75
10.5. eIDAS Qualified ..... 77
10.5.1. eIDAS Qualified Certificate issued to a Natural Person on a QSCD ..... 77
10.5.2. eIDAS Qualified Certificate issued to a Natural Person ..... 79
10.5.3. eIDAS Qualified Certificate issued to a Legal Person on a QSCD ..... 80
10.5.4. eIDAS Qualified Certificate issued to a Legal Person ..... 83
10.5.5. QuoVadis Qualified Website Authentication Certificate (QEVCP-w) ..... 85
10.5.6. QuoVadis QCP-w-psd2 ..... 89
10.6. ZertES Qualified and REGulated ..... 92
10.6.1. Swiss Qualified Certificate ..... 92
10.6.2. Swiss Regulated Certificate issued to a Natural Person ..... 94
10.6.3. Swiss Regulated Certificate issued to a Legal Person (Company Seal) ..... 95
10.7. QV Closed Community ..... 97
10.7.1. Grid Certificates ..... 97
10.8. QuoVadis Device ..... 100
10.9. TLS Certificates ..... 101
10.9.1. OV - Business TLS ..... 101
10.9.2. EV - Extended Validation TLS ..... 103
10.10. Code Signing ..... 110

# 1. INTRODUCTION

## *1.1. OVERVIEW*

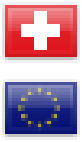
This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that DigiCert Europe (also known as QuoVadis) uses in the generation, issue, use, and management of Certificates and serves to notify Subscribers and Relying Parties of their roles and responsibilities concerning Certificates.

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 Trustlink BV is a Qualified Trust Service Provider (TSP) listed on the Trusted List for the Netherlands, DigiCert Europe Belgium BV (previously QuoVadis Trustlink BVBA) for Belgium and QuoVadis Schweiz AG for Switzerland.

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

In addition a *QuoVadis PKI Disclosure Statement,* which summarises information about the QuoVadis PKI, may be found in the QuoVadis Repository.

| | |
|---|---|
|  | With the exception of CAs issuing Qualified Certificates in accordance with the European eIDAS Regulation, or Swiss Qualified/Regulated Certificates in accordance with Swiss Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing CA and RA services within the QuoVadis PKI.<br><br>Trust service components for EU Qualified Certificates or Swiss Qualified/Regulated Certificates may only be performed by QuoVadis-approved entities that have the relevant certifications. When trust service components are provided by another party QuoVadis maintains overall responsibility and undertakes procedures to ensure that the security and functionality of the trust service meet the appropriate requirements. |

## *1.2. DOCUMENT NAME AND IDENTIFICATION*

This document is the QuoVadis CP/CPS which was adopted by the QuoVadis Policy Management Authority (PMA). The Object Identifiers (OID) assigned to this CP/CPS are defined in Appendix A.

Separate policy documents in the QuoVadis Repository apply to the following QuoVadis Certificates:

- Netherlands PKIoverheid
- QuoVadis Private PKI / Trust Anchor Root CA (1.3.6.1.4.1.8024.0.4)
- BEKB - BCBE Issuing CA G2 (1.3.6.1.4.1.8024.0.3.700.0)
- HIN Health Info Net CA G2 (1.3.6.1.4.1.8024.0.3.800.0)

QuoVadis also operates Time-stamping Authority (TSA) services under a separate QuoVadis Time-Stamp Policy/Practice Statement (OID 1.3.6.1.4.1.8024.0.2000.6).

QuoVadis may include other OIDs as appropriate. OIDs in this list and in QuoVadis certificates belong to their respective owners.

## *1.3. PUBLIC KEY INFRASTRUCTURE PARTICIPANTS*

### 1.3.1. Certification Authorities

QuoVadis operates certification authorities (CAs) that issue digital certificates. As the operator of CAs, QuoVadis performs functions associated with Public Key operations, including receiving Certificate Requests, issuing, revoking, rekeying, and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

Issuing CAs may be operated by QuoVadis or by other Organisations that have been authorised by QuoVadis to participate within the QuoVadis PKI. Issuing CAs are required to ensure that the services they perform within the QuoVadis PKI are in compliance at all times with their respective Issuing CA Agreements and this CP/CPS.

| | |
|---|---|
| | For Qualified Certificates issued out of the itsme Sign Issuing CA, the Registration Service and Subject Device Provisioning Service are not performed by QuoVadis. These services are performed entirely by Belgian Mobile ID, which undergoes its own audit. In addition, some services are shared between QuoVadis and Belgian Mobile ID. QuoVadis retains overall responsibility toward relying parties for all Certificates issued from the of the itsme Sign Issuing CA. |
| | In the case of Qualified Certificates, where QuoVadis manages Key Pairs on behalf of the Subscriber, QuoVadis shall ensure:<br>• where the policy requires the use of a QSCD then the signatures are only created by the QSCD;<br>• in the case of natural persons, the Subscribers' Private Key is maintained and used under their sole control and used only for Electronic Signatures; and<br>• in the case of legal persons, the Subscribers' Private Key is maintained and used under their control and used only for Electronic Seals. |

An Issuing CA may, but shall not be obliged to, detail its specific practices and other requirements in a policy or practices statement adopted by it following approval by the QuoVadis PMA. Issuing CAs are required to conduct regular compliance audits of their RAs to ensure that they are complying their respective RA Agreements and this CP/CPS.

Issuing CAs 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.

External 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 QuoVadis Repository.

*See* also Section 9.6.1.

### 1.3.2. Registration Authorities and Other Delegated Third Parties

A Registration Authority (RA) is an entity that performs Identification and Authentication of Certificate Applicants, and initiates, passes along revocation requests for end user Subscriber Certificates, and approves applications for renewal or re-keying Certificates on behalf of an Issuing CA. QuoVadis and Issuing CAs may act as RAs for Certificates they issue.

RAs may be authorised by QuoVadis to delegate the performance of certain functions to third party validators if it meets the requirements of the QuoVadis CP/CPS. QuoVadis contractually obligates each RA and delegated third party to abide by the policies and industry standards that are applicable to their responsibilities. Where required by a Certificate Class, QuoVadis only allows the use of identity validation methods that have been approved by the relevant Supervisory Authority. Validation of Domains and IP Addresses for TLS and of email addresses included in Certificate Subject fields cannot be delegated.

Third parties, who enter into a contractual relationship with QuoVadis, may act as Enterprise RAs (ERAs) and authorise the issuance of Certificates by QuoVadis for Organisations and Domains that have been pre-

authenticated by QuoVadis. ERAs must abide by all the requirements of this CP/CPS, Section 1.3.2.1 of the S/MIME BR, and the terms of their services agreement with QuoVadis.

*See* also Section 9.6.2.

### 1.3.3. Subscribers

Subscribers use QuoVadis' services and PKI to support transactions and communications. Subscribers under this CP/CPS include all end users (including entities) of Certificates issued by an Issuer CA. A Subscriber is the entity named as the end-user Subscriber of a Certificate. End-user Subscribers may be individuals, organisations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an organisation.

Subscribers are not always the party identified in a Certificate. The *Subject* of a Certificate is the party named in the Certificate. A Subscriber, as used herein, may refer to the Subject of the Certificate and the entity that contracted with QuoVadis for the Certificate's issuance, or the individual responsible for requesting and a Certificate on a trusted system. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

Subscribers are required to act in accordance with this CP/CPS and Subscriber Agreement. *See* also Section 9.6.3.

### 1.3.4. Relying Parties

Relying Parties are entities that act in Reasonable Reliance on a Certificate and/or Digital Signature issued by QuoVadis. A Relying Party may, or may not, also be a Subscriber of the QuoVadis PKI. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the Certificate Status service is detailed within the Certificate.

Relying Parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. *See* also Section 9.6.4.

### 1.3.5. Other Participants

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable agreements. Other participants include Accreditation Authorities such as Policy Management Authorities, Application Software Vendors, and applicable Community-of-Interest sponsors. Accreditation Authorities are granted an unlimited right to re-distribute QuoVadis' Certificates and related information in connection with the accreditation.

## *1.4. CERTIFICATE USAGE*

At all times, participants in the QuoVadis PKI are required to utilise Certificates in accordance with this QuoVadis CP/CPS and all applicable laws and regulations.

### 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. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CP/CPS.

### 1.4.2. Prohibited Certificate Usage

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CP/CPS when the Certificate was issued. Code signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

QuoVadis Certificates shall be used only to the extent the use is consistent with applicable law or regulation, and in particular shall be used only to the extent permitted by applicable export or import laws. CA Certificates subject to the Mozilla Root Store Policy will not be used for any functions except CA functions. In addition, end-user Subscriber Certificates cannot be used as CA Certificates.

QuoVadis may periodically re-key Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed.

QuoVadis strongly discourages key pinning and does not consider it a sufficient reason to delay revocation. Customers should also take care in not mixing Certificates trusted for the web with non-web PKI. Any Certificates trusted by Application Software Vendors must comply with all requirements of all applicable root distribution policies, including revocation periods described in Section 4.9.

## *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).

### 1.5.2. Contact Person

Enquiries or other communications about this CP/CPS should be addressed to the QuoVadis PMA, DigiCert Bermuda Limited, 11 Bermudiana Road, Suite 1640, Hamilton HM-08, Bermuda.

Website: https://www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com
Customer complaints: qvcomplaints@digicert.com

#### *1.5.2.1. Revocation Reporting Contact Person*

QuoVadis provides additional information for entities requiring assistance with revocation or an investigative report at https://www.quovadisglobal.com/certificate-revocation.

For anyone listed in Section 4.9.2 of this CPS and the TLS BR that requires assistance with revocation or investigative reports, QuoVadis provides this page for reporting and submitting requests with all of the necessary information as outlined in Section 4.9: https://problemreport.digicert.com/

If the problem reporting page is unavailable, there is a system outage, or you believe our findings are incorrect please contact revoke@digicert.com. During office hours (CET), problem reports and revocation requests can also be made using the QuoVadis RA and support line +31 (0) 30 232 4320. Outside of office hours CET the emergency revocation hotline can be used at +1 651 229 3456. Typically, the following information is required:

- Common Name
- Certificate serial number
- E-mail address of the Subject

Entities submitting Certificate revocation requests must explain the reason for requesting revocation. QuoVadis or an RA will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. QuoVadis will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorised representative of the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Affiliated Organisation, QuoVadis or an RA will investigate the alleged basis for the revocation request prior to taking action. *See* also Section 4.9.1 and 4.9.3.

### 1.5.3. Person Determining The CP/CPS Suitability

The QuoVadis PMA determines the suitability and applicability of this CP/CPS based on the results and recommendations received from an independent auditor. The PMA is also responsible for evaluating and acting upon the results of compliance audits.

### 1.5.4. CP/CPS Approval Procedures

Approval of this CP/CPS and any amendments hereto is by the QuoVadis PMA. Amendments may be made by updating this entire document or by addendum. The QuoVadis PMA, at its sole discretion, determines whether changes to this CP/CPS require notice or any change in the OID of a Certificate issued pursuant to this CP/CPS. *See* also Section 9.10 and Section 9.12. Any changes to this CP/CPS that relate to Grid topics (refer to Section 10.6.1 below) should be approved by the relevant Grid PMA.

## *1.6. DEFINITIONS AND ACRONYMS*

### 1.6.1. Definitions

**Advanced Electronic Signature**: An Electronic Signature which meets the requirements set out in Article 26 of the eIDAS Regulation.

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

**Application Software Supplier**: A software developer whose software displays or uses QuoVadis Certificates and distributes QuoVadis' Root Certificates.

**Attestation:** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

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

**Authorisation Domain Name**: The Domain Name used to obtain authorisation for certificate issuance for a given FQDN as defined by the TLS BR.

**CAA**: Certification Authority Authorization as defined in RFC 8659.

**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 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 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 Subscriber Agreements on behalf of the Applicant.

**Cryptographic Module**: Secure software, device or utility that (i) generates Key Pairs; (ii) stores cryptographic information; and/or (iii) performs cryptographic functions.

**Digital Certificate**: A digital identifier within the QuoVadis PKI that: (i) identifies the Issuing CA; (ii) identifies the Holder; (iii) contains the Holder's Public and Private Keys; (iv) specifies the Certificate's Operational Term; is digitally signed by the Issuing CA; and (vi) has prescribed Key Usages and Reliance

Factor that governs its issuance and use whether expressly included or incorporated by reference to this CP/CPS.

**Domain Name**: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

**eIDAS Regulation** or eIDAS: Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

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

**Key Pair**: A Private Key and associated Public Key .

**Mailbox Address:** An Email Address as specified in Section 4.1.2 of RFC 5321 and amended by Section 3.2 of RFC 6532, with no additional padding or structure.

**National Competent Authority**: A national authority responsible for payment services. The NCA approves or rejects authorisations for Payment Service Providers in its country.

**Personal Name**: A name of an Individual Subject. The Personal Name may be in a format preferred by the Subject, the CA, or Enterprise RA as long as it remains a meaningful representation of the Subject's verified name.

**Policy Management Authority** (PMA): The QuoVadis body responsible for overseeing and approving CP/CPS amendments and general management.

**Private Key**: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

**Public Key**: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**Qualified Certificate**: A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Certificate meets the qualification requirements defined by the applicable legal framework of the eIDAS Regulation. A Qualified Website Authentication Certificate is a TLS Certificate.

**Qualified Certificate for Electronic Signature:** A Certificate for Electronic Signatures, that is issued by a QTSP and meets the requirements laid down in Annex I of the eIDAS Regulation.

**Qualified Certificate for Electronic Seal:** A Certificate issued to a Legal Person (company) by a QTSP and is used to secure authenticity, integrity and confidentiality in electronic communication of messages and documents.

**Qualified Electronic Signature:** An Advanced Electronic Signature that is created by a QSCD and which is based on a Qualified Certificate for Electronic Signatures.

**Qualified Electronic Signature/Seal Creation Device** (QSCD): An Electronic Signature/seal creation device that meets the requirements laid down in Annex II of eIDAS.

**Qualified Trust Service Provider** (QTSP): A trust service provider which is granted Qualified status by the relevant Supervisory Authority of an EU country under the eIDAS Regulation. A Qualified TSP's Approved Qualified services are shown on an EU Trusted List.

**Regulated Electronic Signature:** An Advanced Electronic Signature which has been created using a secure signature creation unit as referred to in Article 6 of ZertES and is based on a Regulated Certificate issued to a natural person and valid at the time the Electronic Signature is generated.

**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**: An Individual or Organisation that has entered into a Relying Party Agreement authorising that person or Organisation to exercise Reasonable Reliance on Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

**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.

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

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

**Subscriber Agreement**: An agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

**Subscriber**: The entity identified as the Subject in the Certificate.

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

**Terms and Conditions:** The Master Services Agreement, Certificate Terms of Use (or the Qualified Certificate Terms of Use), Privacy Policy, and relevant QuoVadis CP/CPS. The Master Services Agreement references and makes the Certificate Terms of Use, Privacy Policy and relevant QuoVadis CP/CPS part of the Terms and Conditions. The itsme Issuing CA provides its own Terms and Conditions.

### 1.6.2. Acronyms

| | |
|---|---|
| ADN | Authorisation Domain Name |
| ALPN | TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737 |
| CA | Certificate Authority or Certification Authority |
| CAA | Certificate Authority Authorisation |
| CP/CPS | Certificate Policy & Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| CT | Certificate Transparency |
| eIDAS | Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market |
| ERA | Enterprise Registration Authority |
| ETSI | European Telecommunications Standards Initiative |
| EUTL | EU Trusted List |
| EV | Extended Validation |
| FIPS | Federal Information Processing Standard |
| FQDN | Fully Qualified Domain Name |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IETF | Internet Engineering Task Force |
| IGTF | International Grid Trust Federation |
| ITU | International Telecommunication Union |
| LRA | Local Registration Authority |
| NCA | National Competent Authority |

| | |
|---|---|
| OID | Object Identifier |
| OCSP | Online Certificate Status Protocol |
| PKCS | Public Key Cryptography Standard |
| PKI | Public Key Infrastructure |
| PKIX | IETF Working Group on Public Key Infrastructure |
| PMA | QuoVadis Policy Management Authority |
| Portal | Certificate Management System |
| PSD2 | Payment Services Directive - Directive (EU) 2015/2366 |
| PSP | Payment Service Provider |
| QSCD | Qualified Electronic Signature/Seal Creation Device |
| QWAC | Qualified Website Authentication Certificate |
| RA | Registration Authority |
| S/MIME | Secure MIME (Multipurpose Internet Mail Extensions) |
| SSL | Secure Sockets Layer |
| SSCD | Signature/Seal Creation Device |
| TLS | Transaction Layer Security |
| UTC | Coordinated Universal Time |
| X.509 | The ITU-T standard for Certificates and their corresponding authentication framework |

### 1.6.3. References

This CP/CPS describes the practices used to comply with the current versions of the following policies, standards, and requirements as relevant.

| **Standards / Law** | |
|---|---|
| CA/Browser Forum | • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("TLS Baseline Requirements" or "TLS BR"),") and Network and Certificate System Security Requirements published at http://www.cabforum.org<br>• Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines")<br>• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ("S/MIME Baseline Requirements" or "S/MIME BR")<br>• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("CS Baseline Requirements") |
| WebTrust | • WebTrust Principles and Criteria for Certification Authorities<br>• WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security<br>• WebTrust for Certification Authorities – Extended Validation SSL<br>• WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates<br>• WebTrust for Certification Authorities – S/MIME Certificates |

| **Standards / Law** | |
|---|---|
| SR 943.03 [ZertES] | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016 |
| SR 943.032 [VZertES] | Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016 |
| SR 943.032.1 [TAV] | R 943.032.1 / Anhang: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate Ausgabe 1: 23.11.2016<br>Inkrafttreten: 1.1.2017 |
| ETSI EN 319 401 | General Policy Requirements for Trust Service Providers |
| ETSI EN 319 411-1 | Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements |
| ETSI EN 319 411-2 | Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates |
| ETSI EN 319 411-6 | Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates |
| ETSI EN 319 421 | Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps |
| ETSI EN 319 412-1 | Certificate Profiles; Part 1: Overview and common data structures |
| ETSI EN 319 412-2 | Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons |
| ETSI EN 319 412-3 | Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons |
| ETSI EN 319 412-4 | Certificate Profiles; Part 4: Certificate profile for web site certificates |
| ETSI EN 319 412-5 | Certificate Profiles; Part 5: QCStatements |
| ETSI EN 319 422 | Time stamping protocol and electronic time-stamp profiles |
| ETSI TS 119 431-1 | Policy and security requirements for Trust Service Providers; Part 1: TSP service components operating a remote QSCD / SCDev |
| ETSI TS 119 461 | Policy and security requirements for trust service components providing identity proofing of trust service subjects |
| ETSI TS 119 495 | Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 |
| CEN EN 419 241-1 | Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements |
| CEN TS 419 261 | Security requirements for trustworthy systems managing certificates and time-stamps |
| EUGridPMA | Accredited CA by the EU Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) |
| PKIoverheid | Accredited Certification Service Provider under PKIoverheid. PKIoverheid is the name for the PKI designed for trustworthy communication within and with the Dutch Government |

| Standards / Law | |
|---|---|
| Bermuda Authorised Certificate Service Provider | As defined in Bermuda's Electronic Transactions Act 1999 |
| Application Software Vendor | Adobe Approved Trust List Technical Requirements, v.2.0<br>Apple Root Store Program<br>Microsoft Trusted Root Store (Program Requirements)<br>Mozilla Root Store Policy<br>Chromium Project Root Store Certificate Policy |

In the event of any inconsistency between this CP/CPS and the normative provisions of the foregoing Applicable Requirements, then those Applicable Requirements take precedence over this document.

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## *2.1. REPOSITORIES*

QuoVadis provides public repositories for its CA Certificates, revocation data for issued Certificates, CP/CPS, Terms and Conditions, and other important policy documents. The QuoVadis Repository is located at https://www.quovadisglobal.com/repository.

QuoVadis develops, implements, enforces, and updates this CPS at least every 365 days to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. As standards are updated, QuoVadis reviews the changes to determine their impact on these practices. Each section impacted by the standards will be updated and provided to the PMA for approval and implementation.

QuoVadis may register TLS Certificates with publicly accessible Certificate Transparency (CT) Logs. Once submitted, Certificate information cannot be removed from a CT Log.

QuoVadis' CA Certificates, CRLs and OCSP responses are regularly accessible online with systems described in Section 5.

## *2.2. PUBLICATION OF CERTIFICATE INFORMATION*

QuoVadis publishes a Repository that lists all Certificates that have been issued or revoked. Where a Certificate including an email address is issued, the Subscriber consents for the Certificate to be published in the Repository available for Relying Parties to download. The location of the Repository and OCSP responders are given in the individual Certificate Profiles more fully disclosed in Appendix A and Appendix B to this CP/CPS.

QuoVadis hosts test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate at https://chain-demos.digicert.com/

## *2.3. TIME OR FREQUENCY OF PUBLICATION*

QuoVadis publishes CRL and OCSP resources to allow Relying Parties to determine the validity of a QuoVadis Certificate. Certificate information is published promptly following generation and issue and immediately following the completion of the revocation process.

QuoVadis updates this CP/CPS at least annually to describe how QuoVadis meets the requirements of standards referred to in Sections 1.1 and 1.6.3 including the TLS BR and S/MIME BR. Those updates indicate conformance by incrementing the version number and adding a dated changelog entry even if no other changes are made to the document as specified in Section 1.2 of this CP/CPS

New or modified versions of the CP/CPS and other policies are typically published within seven days after their approval.

## *2.4. ACCESS CONTROLS ON REPOSITORIES*

Read-only access to the Repository is unrestricted and is available 24 x 7. Logical and physical controls prevent unauthorised write access to Repositories. In the event that the Repository is unavailable then QuoVadis aims to restore availability within 24 hours.

# 3. IDENTIFICATION AND AUTHENTICATION

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

## *3.1. NAMING*

### 3.1.1. Types Of Names

All Subscribers require a distinguished name that complies with the ITU X.500 standard for Distinguished Names (DN). The QuoVadis PMA approves naming conventions for the creation of distinguished names for Issuing CA applicants. Different naming conventions may be used by different Issuing CAs.

Names consisting of multiple words are permitted. Subjects MAY chose name order in accordance with national preference.

Each User must have a unique and readily identifiable Subject DN. Alternatively, DNs may be based on domain name components, e.g. CN=John Smith, DC=QuoVadis, DC=BM. The Common Name may contain the applicant's first and last name (surname).

For Certificates issued under the TLS BR, the use of Internal Server Names and Reserved IP Addresses is prohibited, and the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and/or the Subject Alternative Name extension. Wildcard TLS 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 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.

### 3.1.2. Need For Names To Be Meaningful

QuoVadis uses Distinguished Names that identify both the entity (i.e. person, organisation, device, or object) that is the Subject of the Certificate and the entity that is the issuer of the Certificate. QuoVadis only allows directory information trees that accurately reflect organisation structures. Personal Names included in Certificates issued to Individuals shall be a meaningful representation of the authenticated common name of the Subscriber.

### 3.1.3. Pseudonymous Subscribers

QuoVadis may issue pseudonymous end entity Certificates if they are not prohibited by policy and if applicable name space uniqueness requirements are met. QuoVadis requires identification of the real identity of the Applicant in accordance with Section 3.2.3. The pseudonym shall be either a unique identifier selected by QuoVadis for the Subject of the Certificate, or an identifier selected by an Enterprise RA which uniquely identifies the Subject of the Certificate within the organisation.

### 3.1.4. Rules For Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. QuoVadis may allow the conversion of Identity information usually rendered in non-ASCII characters (for example é and à may be represented by e or a, and umlauts such as ö or ü may be represented by oe or ue, o or u respectively). QuoVadis may use language variants (such as Munich or München) for geographic names. For Personal Names, QuoVadis include an ASCII character name that is not a direct Conversion of the Applicant's registered name provided that it is verified in a Reliable Data Source or suitable Attestation.

### 3.1.5. Uniqueness Of Names

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

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

### 3.1.6. Recognition, Authentication, And Role Of Trademarks

Unless otherwise specifically stated in this CP/CPS, QuoVadis does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. QuoVadis may reject any application or require revocation of any Certificate that is part of a trademark dispute.

## *3.2. INITIAL IDENTITY VALIDATION*

QuoVadis may use any legal means of communication or investigation to ascertain the identity of an organisational or individual Applicant in compliance with this CP/CPS. QuoVadis may refuse to issue a Certificate in its sole discretion.

### 3.2.1. Method To Prove Possession Of Private Key

Issuing CAs shall establish that each Applicant for a Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the request for a Certificate. The Issuing CA shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol, including PKCS#10. This requirement does not apply where a Key Pair is generated on behalf of a Subscriber.

### 3.2.2. Authentication Of Organisation Identity

The Identity of an Organisation (legal person) is required to be authenticated with respect to each Certificate that asserts (i) the identity of an Organisation; or (ii) an Individual, system, device, or other organisational entity's affiliation with an Organisation. Without limitation to the generality of the foregoing, the Identity of any Organisation that seeks to act as a RA for its employees and/or employees of its respective Subsidiaries, Holding Companies or Counterparties is required to be authenticated.

In order to authenticate the Identity of an Organisation, evidence shall be provided of:

i) Full name of the legal person;

ii) Reference to a nationally recognised registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name; and

iii) When applicable, the association between the legal person and any other organisational entity identified in association with this legal person that would appear in the Organisation attribute of the Certificate, consistent with the national or other applicable identification practices.

At a minimum, confirmation is required that: (i) the Organisation legally exists in the name that will appear in the DN of any Certificates issued under its name, or is legally recognised as doing business under an alternative proposed by the Organisation; and (ii) all other information contained in the Certificate application is accurate.

Registration information provided by an Organisation may be validated by reference to official government records and/or information provided by a reputable vendor of corporate information services. Additional information is provided in *Acceptable Sources for QuoVadis Authentication of Identity* in the QuoVadis Repository. The accuracy and currency of such information may be validated by conducting checks with financial institution references, credit reporting agencies, trade associations, and other entities that have continuous and ongoing relationships with the Organisation under review. In addition, the telephone number

provided by the Organisation as the telephone number of its principal place of business may be called to ensure that the number is active and answered by the Organisation.

Where an Issuing CA or RA has a separate and pre-existing commercial relationship with the Organisation under review, the Issuing CA or RA may authenticate the Identity of the Organisation by reference to records kept in the ordinary course of business that, at a minimum, satisfy the requirements of this Section. In all such cases, the Issuing CA or RA shall record the specific records upon which it relied for this purpose.

For Certificates issued to a natural person representing a legal person, address information included in the DN may be that of the sponsoring Organisation.

With respect to TLS Certificates, authentication of Organisation identity is conducted in compliance with this CP/CPS and the TLS BR.

With respect to S/MIME Certificates, authentication of Organisation identity is conducted in compliance with this CP/CPS and the S/MIME BR.

When a subject:organizationIdentifer is included in Qualified or Regulated Certificates, the organizationIdentifer is formatted in accordance with Section 5.1.4 of ETSI EN 319 412-1 for Qualified or Regulated Certificates and in accordance with the S/MIME BR for S/MIME Certificates.

QuoVadis uses a documented internal process to check the accuracy of information sources and databases to ensure the data is acceptable, including reviewing the database provider's terms of use. A list of the approved sources/Trusted Registers is published in a file linked at https://github.com/digicert/reports/tree/master/validation-sources.

QuoVadis may include the Legal Entity Identifier (LEI) numbers in Certificates after verification through appropriate mechanisms, such as provided by Global Legal Entity Identifier Foundation (GLEIF), that the LEI is associated with the Subject. LEI lookups are not relied upon by QuoVadis as a primary source of information for verification and this information is treated as additional correlation of identity information found in the certificate.

#### *3.2.2.1. Validation of Domain and Email Authorisation and Control*

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

i) TLS BR Section 3.2.2.4.1 is no longer used as it is deprecated as of August 1, 2018;

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

iii) TLS BR Section 3.2.2.4.3 is no longer used because it is deprecated as of May 31, 2019;

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

v) TLS BR Section 3.2.2.4.5 is no longer used because it is deprecated as of August 1, 2018;

vi) TLS BR Section 3.2.2.4.6 is no longer used because it is deprecated as of April 24, 2020;

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

viii) 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 TLS BR Sections 3.2.2.5 and 3.2.2.4.8;

ix) TLS BR Section 3.2.2.4.9 is no longer used because it was deprecated as of March 16, 2019;

x) TLS BR Section 3.2.2.4.10 is no longer used because it was deprecated as of September 22, 2020;

xi) TLS BR Section 3.2.2.4.11 is no longer used because it is deprecated as of February 5, 2018;

xii) TLS BR Section 3.2.2.4.12 is not used by QuoVadis;

xiii) 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 utilising the Random Value. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance with BR Section 3.2.2.4.13;

xiv) Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the ADN and then receiving a confirming response utilising the Random Value, performed in accordance with TLS BR Section 3.2.2.4.14;

xv) Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call can confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with TLS BR Section 3.2.2.4.15;

xvi) 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 ADN. Each phone call can confirm control of multiple ADN provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with TLS BR Section 3.2.2.4.16;

xvii) Confirming the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response. Each phone call can confirm control of multiple domains provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and a confirming response is provided for each ADN. Performed in accordance with TLS BR Section 3.2.2.4.17;

xviii) Confirming the Applicant's control over the requested FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token,Random Value that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request). Performed in accordance with TLS BR Section 3.2.2.4.18; and

xix) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method, performed in accordance with TLS BR Section 3.2.2.4.19 and Section 8.3 of RFC 8555 as prescribed; or

xx) TLS BR Section 3.2.2.4.20 is not used by QuoVadis.

Wildcard Domain Name validation is completed using the above list as permitted by the TLS BR along with current best practice of consulting a public suffix list.

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. Verification of Email*

QuoVadis and its Issuing CAs verify an Applicant's or Organisation's right to use or control of a Mailbox Address to be included in a Certificate that will have the id-kp-emailProtection EKU using one of the following procedures, which may not be delegated:

i) By verifying domain control over the email Domain Name using one of the procedures listed in this Section in accordance with S/MIME BR Section 3.2.2.1; or

ii) By sending an email message containing a unique Random Value to the Mailbox Address to be included in the Certificate and receiving a confirming response within 24 hours that includes the Random Value to indicate that the Applicant controls that same Mailbox Address, in accordance with S/MIME BR Section 3.2.2.2; or

iii) By confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed, in accordance with S/MIME BR Section 3.2.2.3.

#### *3.2.2.3. Verification of IP Address*

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

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

ii) 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 utilising the Random Value, performed in accordance with TLS BR Section 3.2.2.5.2;

iii) Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with TLS BR Section 3.2.2.5.3;

iv) TLS BR Section 3.2.2.5.3 is no longer used because it was deprecated as of July 31, 2019.

v) Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address RA, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with TLS BR Section 3.2.2.5.5;

vi) 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 TLS BR Section 3.2.2.5.6; or

vii) TLS BR Section 3.2.2.5.7 is not used by QuoVadis

#### *3.2.2.4. Wildcard Domain Validation*

Before issuing a TLS Certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, QuoVadis follows a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix". If a wildcard would fall within the label immediately to the left of a registry-controlled /1 or public suffix, QuoVadis refuses issuance unless the Applicant proves its rightful control of the entire Domain Namespace.

#### *3.2.2.5. Verification of Country*

If the Applicant requests a publicly-trusted TLS Certificate that will contain the countryName field and other Subject Identity Information, then QuoVadis verifies the identity of the Applicant, and the authenticity of the Applicant Representative's Certificate Request using a verification process meeting the requirements of Section 3.2.2.1 in the TLS BR and this Section. QuoVadis inspects any document relied upon for alteration or falsification.

### 3.2.3. Authentication Of Individual Identity

An Individual's Identity is to be authenticated in accordance with this CP/CPS and the Certificate Class together with the relevant application data and documentation. QuoVadis TLS Certificates are only issued to Organisations and not natural persons. By requesting a QuoVadis Certificate, an Applicant accepts to undertake one of the following identity proofing methods and the related terms and conditions.

QuoVadis authenticates an Individual's Identity and, if applicable, any specific attributes using the following methods:

- Physical presence;
- Remote identity verification means which provide equivalent assurance in terms of reliability to the physical presence;
- Reliance on an Electronic Signature; and/or
- Video verification.

*See* Appendix A for additional information on the authentication methods that are available for each Certificate Class. QuoVadis only allows the use of identity validation methods that have been approved by the relevant Supervisory Authority.

If the Subject is a natural person, evidence shall be provided to deliver unique identification of the Applicant, including:

i) Full name (including surname and given names consistent with applicable law and national identification practices); and

ii) Date and place of birth, or reference to at least one nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Subject is a natural person identified in association with an organisational entity (legal person), additional evidence shall be provided of:

i) Full name and legal status of the associated organisational entity;

ii) Any relevant existing registration information (e.g. company registration) of the organisational entity; and

iii) Evidence that the Subject is affiliated with the organisational entity which may include reference to an attestation or a Trusted Register. Attestations may be made by directors, executives, board members, or a natural person with authorisation duly delegated from another natural person in an authorised role.

Enterprise RA records may be used to verify Individual Identity attributes, including pseudonyms, included in Sponsor-validated Certificates issued within the ERA's Organisation in accordance with the S/MIME BR.

The current validity must be established of any Attestation or document regarding a natural person's relationship to a legal person. The role and authorisation of the natural person providing such Attestation or document shall be recorded.

At least one digital or physical identity document shall be used as authoritative evidence. Identity documents must be valid at the time of proofing. Acceptable identity documents must contain a face photo and/or other information that can be compared with the Applicant's physical attributes. If physical identity documents are used as evidence, the documents shall be presented in their original form by the Subject of the identity proofing. If digital identity documents are used as evidence, only eMRTD (Electronic Machine Readable Travel Documents) according to ICAO 9303 part 10 and other digital documents that offer comparable reliability of the identity shall be accepted.

The Trusted Registers and identity documents (such as passports and national identity cards) accepted in QuoVadis verification procedures are identified in *Acceptable Sources for QuoVadis Authentication of Identity* in the QuoVadis Repository.

Identity proofing may use additional digital or physical identity documents, Trusted Registers, proof of access, or other documents and Attestations as supplementary evidence. Only official national or nationally approved registers are accepted as Trusted Registers.

By loading or using identity proofing software provided by QuoVadis, Applicants agree that such use will be subject to the terms and conditions of the Master Services Agreement. Use of the software may also be subject to additional terms between the Applicant and the identity proofing software provider.

#### *3.2.3.1. Physical Presence*

In-person (manual) verification requires the physical presence of the Applicant in order to conduct the identity proofing, to validate the identity document, and to bind the identity to the Applicant. The Applicant is not required to be present for all steps of the verification, which may include manual procedures, the use of automated procedures (including identity proofing software), or a hybrid approach using manual and automated procedures.

Entities that can perform this verification include the CA or RA, a Public Official or third-party validator approved by QuoVadis, or a registered Notary. In some cases, a delegated RA such as an Enterprise RA may

confirm attributes where Certificates may assert the Individual's affiliation with an Organisation or rely upon previously conducted procedures, accepted Know Your Customer (KYC) standards, or a contractual relationship with the RA.

#### *3.2.3.2. Remote Identity Verification*

Remote Identity Verification allows the Applicant to use identity proofing software to assist in automating the proofing and validation of either physical or digital identity documents and the binding to the Applicant.

Depending on the requirements of the Certificate Class, Remote Identity Verification may include fully automated procedures or a hybrid approach using manual and automated procedures.

Where required by a Certificate Class, QuoVadis only accepts Remote Identity Verification following review and acceptance of the method by the relevant Conformity Assessment Body and/or Supervisory Authority. In such cases, the Remote Identity Verification method used by QuoVadis has an assurance level of 'Substantial' or 'High' as set out in Article 8 of the eIDAS Regulation.

QuoVadis supports four levels of Remote Identity Verification:

| **Level** | **Description** |
|---|---|
| RIV1 | Base RIV plus manual review in defined cases (e.g, fraud risk, changes made by RA) |
| RIV2 | Base RIV plus manual review in all cases |
| RIV3 | Base RIV plus NFC Authentication with manual review in defined cases (e.g, fraud risk, changes made by RA) |
| RIV4 | Base RIV plus NFC Authentication with manual review in all cases |

Base RIV includes OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options include read of eMRTD data, Passive Authentication, and Active Authentication. Information collected and verified may include:

| | | |
|---|---|---|
| First name | ID number | ID issuance date |
| Last name | ID valid until | Issuing authority |
| Phone number | Scan of ID Document | Image of face |
| Email | Place of birth | Street |
| Date of birth | Nationality | Zipcode |
| ID type | Issuing country | City |
| Title | | |

Entities that can perform this verification include the CA, RA, or third-party validators approved by QuoVadis.

#### *3.2.3.3. Reliance On Electronic Signature*

QuoVadis may rely upon an existing digital signature with a supporting Certificate as evidence. The digital signature can be applied by a natural person (electronic signature as defined by eIDAS), a legal person (electronic seal as defined by eIDAS), or a natural person representing a legal person. For Qualified Certificates, QuoVadis shall rely upon a Qualified Electronic Signature created as part of the identity proofing process in order to verify an Applicant's identity and additional attributes if the currently valid Certificate was issued by QuoVadis, or by another Issuing CA, following validation of the Certificate using the relevant Trusted List.

Entities that can perform this verification include the CA or RA.

#### *3.2.3.4. Video Verification*

QuoVadis may also use video-based verification procedures where the Applicant interacts with an RA via a web video session or identity proofing software. Depending on the requirements of the Certificate Class, video identification may include manual or automated procedures, or a hybrid of both including video capture, biometric comparison, scanning of identity documents, liveness checks, and other tools.

Where required by a Certificate Class, QuoVadis only accepts remote video verification following review and acceptance of the method by the relevant Conformity Assessment Body and/or Supervisory Authority.

Entities that can perform this verification include the CA, RA, or third-party validators approved by QuoVadis.

### 3.2.4. Non-Verified Subscriber Information

QuoVadis does not verify information contained in the Organisation Unit (OU) field in Certificates. Other information may be designated as non-verified according to the Certificate Profile or relevant industry standards. As of August 31, 2020 QuoVadis does not include OU fields in TLS Certificates.

### 3.2.5. Validation Of Authority

Where an Applicant's Name is to be associated with an Organisational Name to indicate his or her status as a Counterparty, Employee or specifies an Authorisation level to act on behalf of an Organisation, the RA will validate the Applicant's Authority by reference to business records maintained by the RA, its Subsidiaries, Holding Companies or Affiliates. Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix A. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

An Organisation may limit who is authorised to request Certificates by sending a request to QuoVadis. A request to limit authorised individuals is not effective until approved by QuoVadis. QuoVadis will respond to an Organisation's verified request for QuoVadis' list of its authorised requesters.

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

### 3.2.6. Criteria for Interoperation

QuoVadis may provide interoperation services to certify a non-QuoVadis CA, allowing it to interoperate with the QuoVadis PKI. In order for such interoperation services to be provided the following criteria must be met:

- QuoVadis will perform due diligence on the CA;
- A formal contract must be entered into with QuoVadis, which includes a 'right to audit' clause; and
- The CA must operate under a CPS that meets QuoVadis requirements.

## *3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS*

### 3.3.1. Identification And Authentication For Routine Re-Key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, QuoVadis creates a new Certificate with the same Certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, QuoVadis may perform some revalidation of the Applicant but may also rely on information previously provided or obtained. QuoVadis does not re-key a Certificate without additional Identification and Authentication if doing so would allow the Subscriber to use the Certificate beyond the limits specified for the applicable Certificate Profile.

### 3.3.2. Identification and Authentication For Re-Key After Revocation

QuoVadis does not allow re-key after revocation. To re-key a revoked Certificate, the Subscriber must undergo the initial Identification and Authentication process prior to re-keying the Certificate.

## *3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS*

*See* Section 4.9 for information about Certificate Revocation procedures. All revocation requests are authenticated by QuoVadis or the RA responsible for issuing the Certificate. QuoVadis authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised. A Subscriber may request that their Certificate be revoked by:

- Authenticating to a QuoVadis Portal and requesting revocation via that system;
- Applying in person to the RA, Issuing CA or QuoVadis supplying either original proof of identification in the form of a valid Passport or National ID; or
- Telephonic communication using a pre-existing shared secret, password or other information associated with Subscriber's account with the CA following appropriate Identification.

# 4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

## *4.1. CERTIFICATE APPLICATION*

### 4.1.1. Who Can Submit A Certificate Application

Either the Applicant or an individual authorised to request Certificates on behalf of the Applicant may submit Certificate Requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to QuoVadis

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

The Applicant is responsible to provide correct and up-to-date data, as required for the generation and issuance of Certificates as well as the correct usage of the Certificates. By agreeing to the Master Service Agreement, Terms of Use, and the Privacy Notice and signing the contracts, the Applicant also agrees to all underlying documents (the CP/CPS and others). If any of the required information for the issuance of Certificates is missing, incomplete or produces a negative outcome, QuoVadis will reject the application for a Certificate.

QuoVadis maintains an internal database of previously revoked Certificates and previously rejected Certificate Requests. QuoVadis uses this information to identify subsequent suspicious Certificate Requests .

### 4.1.2. Enrolment Process And Responsibilities

Certificate Requests must be in a form prescribed by the Issuing CA and typically include i) an application form including all registration information as described by this CP/CPS, ii) secure generation of KeyPair and delivery of the Public Key to QuoVadis, (a CSR may not be required), iii) acceptance of the relevant Subscriber Agreement or other Terms of Use upon which the Certificate is to be issued, iv) and payment of fees. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

A Certificate Request may be used for multiple Certificates to be issued to the same Applicant, (subject to the updating requirement in Section 4.2.1 of the TLS BR). The Certificate Request contains a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

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

## *4.2. CERTIFICATE APPLICATION PROCESSING*

### 4.2.1. Performing Identification And Authentication Functions

After receiving a certificate application, QuoVadis or an RA follows a documented procedure to verify the application and other information in accordance with the Identification and Authentication requirements for each Certificate Profile. *See* also Appendix A.

In cases where the Certificate Request does not contain all the necessary information about the Applicant, QuoVadis or the RA obtains the remaining information from the Applicant or, having obtained it from a reliable, independent third-party data source, confirm it with the Applicant.

For publicly-trusted TLS Certificates, Applicant information is required to include at least one FQDN or IP address to be included in the Certificate's SubjectAltName extension. For validation of Domain Names and IP Addresses according to Section 3.2.2.1 and 3.2.2.3 any reused data, document, or completed validation must be obtained no more than 398 days prior to issuing the Certificate. QuoVadis implements documented procedures that require additional verifications as reasonably necessary for High Risk Certificate Requests prior to the Certificate's approval.

For S/MIME Certificates, validation of email control according to Section 3.2.2.2 must be obtained no more than 30 days prior to issuing the Certificate. Authentication of organisational entity of Individual Identity must be obtained no more than 825 days prior to issuing the Certificate.

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

#### *4.2.1.1. Certificate Authority Authorisation (CAA)*

Prior to issuing TLS Certificates, QuoVadis checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued. If the QuoVadis 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 8659. QuoVadis may not act on the contents of the iodef property tag. QuoVadis will not issue a Certificate if an unrecognised property is found with the critical flag.

CAA checking is optional for Certificates issued by a Technically Constrained Issuing CA as set out in TLS BR Section 7.1.5, or where CAA was checked prior to the creation of a corresponding CT pre-certificate that was logged in at least 2 public CT log servers.

DNS access failure can be treated as permission to issue when the failure is proven to be outside QuoVadis infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

QuoVadis documents potential issuances that were prevented by a CAA record, and may not dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. QuoVadis supports mailto: and https: URL schemes in the iodef record.

The identifying CAA domains recognised by QuoVadis: are "digicert.com", "digicert.ne.jp", "cybertrust.ne.jp", "symantec.com", "thawte.com", "geotrust.com", "quovadisglobal.com", "rapidssl.com", "digitalcertvalidation.com" and any domain containing those identifying domains as suffixes (e.g. example.digicert.com) or registered country jurisdictions (e.g., digicert.de).

### 4.2.2. Approval Or Rejection Of Certificate Applications

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

If an RA (including an Enterprise RA) assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of

such performance to QuoVadis. After verification is complete, QuoVadis Validation Specialists evaluate the corpus of information and decides whether or not to approve issuance.

QuoVadis does not issue Certificates containing a new gTLD under consideration by ICANN until the gTLD has been approved. QuoVadis may also reject a Certificate Application if QuoVadis believes that issuing the Certificate could damage or diminish QuoVadis' reputation or business. QuoVadis does not issue publicly trusted TLS Certificates containing unregistered TLD's or when domain control cannot be verified.

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

QuoVadis, in its sole discretion, 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. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the Certificate.

### 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, as well as the availability of Trusted Registers and Attestations. Upon the receipt of the necessary details and documentation, QuoVadis aims to complete the validation process and issue or reject a Certificate Application within three working days. Events outside of the control of QuoVadis may delay the issuance process.

## *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. QuoVadis does not issue end entity TLS Certificates directly from its Root Certificates.

Certificate issuance by a Root CA requires at least two individuals authorised by QuoVadis (i.e. the CA system operator, system officer, or PKI administrator), one of whom deliberately commands the Root CA to perform a Certificate signing operation. Databases and CA processes occurring during Certificate issuance are protected from unauthorised modification.

### 4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate

QuoVadis may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, QuoVadis delivers instructions via email to the Mailbox Address designated by the Certificate Requester during the application process.

### 4.3.3. Notification to NCA for PSD2 Certificates

QuoVadis maintains a register of NCA contact information. When a PSD2 Certificate is issued, QuoVadis will send a notification email to the NCA identified in the Certificate using the pre-registered contact information.

## *4.4. CERTIFICATE ACCEPTANCE*

### 4.4.1. Conduct Constituting Certificate Acceptance

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

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

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

ACCEPTING A CERTIFICATE, THE SUBSCRIBER ASSUMES A DUTY TO RETAIN CONTROL OF THE CERTIFICATE'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS, EXCLUSION, MODIFICATION OR UNAUTHORISED USE.

### 4.4.2. Publication Of The Certificate By The CA

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

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

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

## *4.5. KEY PAIR AND CERTIFICATE USAGE*

### 4.5.1. Subscriber Private Key And Certificate Usage

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

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

### 4.5.2. Relying Party Public Key And Certificate Usage

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

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

A Relying Party should rely on a Digital Signature or TLS handshake only if:

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

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

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

## *4.6. CERTIFICATE RENEWAL*

### 4.6.1. Circumstance For Certificate Renewal

Renewal means the issuance of a new Certificate to the Subscriber without changing the Subscriber or other participant's Public Key or any other information in the Certificate. QuoVadis may renew a Certificate if:

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

ii) the Subscriber and attributes are consistent; and

iii) the associated Private Key remains uncompromised.

QuoVadis may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. QuoVadis may notify Subscribers prior to a Certificate's expiration date. QuoVadis renewal requires payment of additional fees. QuoVadis may renew a certificate after expiration if the relevant industry permits such practices.

### 4.6.2. Who May Request Renewal

Only the Certificate Subject or an authorised representative of the Certificate Subject may request renewal of the Subscriber's Certificates.

### 4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance, but QuoVadis may use previously collected information that is still considered fresh under applicable industry standards. QuoVadis will revalidate any information that is older than the periods specified in applicable standards for the Certificate Policy. QuoVadis may refuse to renew a Certificate if it cannot verify any rechecked information.

### 4.6.4. Notification Of New Certificate Issuance To Subscriber

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

### 4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate

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

### 4.6.6. Publication of the Renewal Certificate By The CA

QuoVadis publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in QuoVadis' Repository.

### 4.6.7. Notification Of Certificate Issuance By The CA To Other Entities

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

## *4.7. CERTIFICATE RE-KEY*

Re-keying means creating a new Certificate with a new Public Key and serial number while keeping the Subject information the same.

### 4.7.1. Circumstance For Certificate Re-Key

Certificates may be re-keyed upon request. After re-keying a Certificate, QuoVadis may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate. Subscribers requesting re-key should identify and authenticate themselves as permitted by Section 3.3.1.

### 4.7.2. Who May Request Re-Key

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

### 4.7.3. Processing Certificate Re-Key Request

If the Private Key and any identity and domain information in a Certificate have not changed, then QuoVadis may issue a replacement Certificate using a previously issued Certificate or previously provided CSR. QuoVadis may re-use existing verification and authentication information in accordance with Section 3.3 unless QuoVadis believes that the information has become inaccurate.

### 4.7.4. Notification Of Certificate Re-Key To Subscriber

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

### 4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate

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

### 4.7.6. Publication Of The Re-Key Certificate By The CA

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

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

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

## *4.8. CERTIFICATE MODIFICATION*

### 4.8.1. Circumstances For Certificate Modification

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

### 4.8.2. Who May Request Certificate Modification

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

### 4.8.3. Processing Certificate Modification Requests

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

### 4.8.4. Notification Of Certificate Modification To Subscriber

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

### 4.8.5. Conduct Constituting Acceptance Of A Modified Certificate

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

### 4.8.6. Publication Of The Modified Certificate By The CA

QuoVadis publishes modified Certificates by delivering them to Subscribers.

### 4.8.7. Notification Of Certificate Modification By The CA To Other Entities

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

## *4.9. CERTIFICATE REVOCATION AND SUSPENSION*

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, QuoVadis and Issuing CAs verify that a revocation request was initiated by Subscribers, an RA, an Issuing CA, and other entities listed in Section 4.9.2 of this CP/CPS. Other parties may submit Certificate Problem Reports to QuoVadis to report

reasonable cause to revoke the Certificate. Issuing CAs are required to provide evidence of the revocation authorisation to QuoVadis upon request.

### 4.9.1. Circumstances For Revocation

QuoVadis will revoke a Certificate within 24 hours after receipt and use the corresponding CRLReason in accordance with Section 7.2, confirming one or more of the following occurred:

i) The Subscriber requests in writing that QuoVadis revoke the Certificate but does not specify a reason (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

ii) The Subscriber notifies QuoVadis that the original Certificate Request was not authorised and does not retroactively grant authorisation (CRLReason #9, privilegeWithdrawn);

iii) QuoVadis obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

iv) QuoVadis obtains evidence that the validation of domain authorisation or control for any FDQN or IP address or mailbox control for any Mailbox Address in the Certificate should not be relied upon (CRLReason #4, superseded);

v) QuoVadis is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);

vi) The NCA requests revocation for a PSD2 Certificate where the Subscriber (PSP) has lost its authorisation to act as a PSP or any PSP role in the Certificate has been removed (CRLReason #9, privilegeWithdrawn); or

vii) QuoVadis has reasonable assurance that a certificate was used to sign suspect code.

In the absence of exceptional circumstances confirmed with the relevant Supervisory Authority, QuoVadis will revoke a Certificate within 24 hours when QuoVadis becomes aware that a QSCD used for QCP-n-qscd or QCP-l-qscd loses its certification status.

QuoVadis may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days after receipt and confirming that one or more of the following occurred:

i) QuoVadis obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement (CRLReason #9, privilegeWithdrawn);

ii) The Subscriber breached a material obligation under the CP/CPS or the relevant agreement (CRLReason #9, privilegeWithdrawn);

iii) QuoVadis confirms any circumstance indicating that use of a FQDN, IP address, or Mailbox 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) (CRLReason #5, cessationOfOperation);

iv) For code signing, the Application Software Vendor requests revocation and QuoVadis does not intend to pursue an alternative course of action;

v) For code signing, the Certificate is being used to sign Suspect Code;

vi) QuoVadis confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);

vii) QuoVadis confirms a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);

viii) QuoVadis confirms that the Certificate was not issued in accordance with the CA/Browser Forum requirements or relevant browser policy (CRLReason #9, privilegeWithdrawn);

ix) QuoVadis determines or confirms that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

x) QuoVadis right to issue Certificates under the CA/Browser Forum requirements expires or is revoked or terminated, unless QuoVadis has made arrangements to continue maintaining the CRL/OCSP Repository for a reason that is not otherwise required to be specified by this Section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL;

xi) Revocation is required by the QuoVadis CP/CPS for a reason that is not otherwise required to be specified by this Section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL;

xii) QuoVadis confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);

xiii) Where the Subscriber becomes unsuitable or unauthorised to hold a Certificate on behalf of an employer or its respective Subsidiaries, Holding Companies or Counterparties (CRLReason #9, privilegeWithdrawn); or

xiv) The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of the Codesigning Baseline Requirements. 13. For Codesigning Certificates, Application Software Suppliers may request the Issuer CA delays revocation where immediate revocation has a potentially large negative impact to the ecosystem

QuoVadis may revoke any Certificate in its sole discretion, including if QuoVadis believes that:

i) Either the Subscriber or QuoVadis obligations under the CP/CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;

ii) QuoVadis received a lawful and binding order from a government or regulatory body to revoke the Certificate;

iii) The Subscriber is confirmed to be bankrupt, in liquidation, or deceased;

iv) QuoVadis ceased operations and did not arrange for another CA to provide revocation support for the Certificates;

v) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers, Relying Parties, or others;

vi) The Subscriber was added as a denied party or prohibited person to a blocklist or is operating from a destination prohibited under the laws of the United States;

vii) For Adobe Signing Certificates, Adobe has requested revocation; or

viii) For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

ix) QuoVadis receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Subscriber that is contained within the Certificate;

x) The Subscriber 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 always revokes a Certificate if the binding between the Subject and the Subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

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

i) The Issuing CA requests revocation in writing;

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

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

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

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

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

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

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

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

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

In the event that an Issuing CA determines that its Certificates or the QuoVadis PKI could become compromised and that revocation of Certificates is in the interests of the PKI, following remedial action, QuoVadis may authorise the reissue of Certificates to Subscribers at no charge, unless the actions of the Subscribers were in breach of the QuoVadis CP/CPS or other contractual documents.

### 4.9.2. Who Can Request Revocation

Any appropriately authorised party may request revocation of a Certificate. This may include a recognised representative of a Subscriber or the RA, the party that purchased the Certificate on behalf of a Subscriber, and the party that manages the Portal account to which the Certificate is tied. QuoVadis may revoke a Certificate without receiving a request and without reason. Third parties may request Certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

QuoVadis provides Anti-Malware Organisations, Subscribers, Relying Parties, Application Software Vendors, and other third parties (such as a National Competent Authority that issued the Authorisation Number in a PSD2 Certificate) with clear instructions on how they can report suspected Private Key compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates at https://problemreport.digicert.com/ and other resources listed in Section 1.5.2.1.

### 4.9.3. Procedure For Revocation Request

QuoVadis processes a revocation request as follows:

i) QuoVadis logs the request or problem report and the reason for requesting revocation based on the list in Section 4.9.1, including contact information for the requestor. QuoVadis may also include its own reasons for revocation in the log.

ii) QuoVadis may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).

iii) If the request is authenticated as originating from the Subscriber or an authorised party, QuoVadis revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.

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

- the nature of the alleged problem;
- the number of reports received about a particular Certificate or website;

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

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

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

QuoVadis maintains a continuous 24x7 ability to internally respond to high priority revocation requests and certificate problem reports at https://problemreport.digicert.com/ and other resources listed in Section 1.5.2.1. Subscribers may also revoke their Certificates via the QuoVadis Portal.

For Certificates issued from an itsme sign Issuing CA all revocation requests must be directed to the itsme first-line helpdesk.

### 4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. No grace period is permitted once a revocation request has been verified. QuoVadis will revoke Certificates as soon as reasonably practical following verification of a revocation request.

### 4.9.5. Time Within Which The CA Must Process The Revocation Request

QuoVadis will revoke a CA Certificate within one hour after receiving clear instructions from the PMA.

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

After reviewing the facts and circumstances, QuoVadis works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which QuoVadis will revoke the Certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by QuoVadis will consider the following criteria:

i) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

ii) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);

iii) The number of Certificate problem reports received about a particular Certificate or Subscriber;

iv) The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

v) Relevant legislation.

The time used for the provision of revocation services is synchronised with UTC at least every 24 hours. Under normal operating circumstances, QuoVadis will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this Section and Section 4.9.1. For Certificates containing the ETSI OIDs defined in Section 10.1.1 the maximum delay between the receipt of the revocation request and the update of the Certificate Status information is at most 24 hours.

For Certificates issued from the itsme sign Issuing CA, this 24 hour time period starts with the receipt of the revocation request at the itsme first-line helpdesk.

QuoVadis follows the revocation timeframes specified for malware in the Code Signing Baseline Requirements.

### 4.9.6. Revocation Checking Requirement For Relying Parties

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

### 4.9.7. CRL Issuance Frequency

QuoVadis uses its offline Root CAs to publish CRLs for its Issuing CAs at least every 6 months and within 18 hours after revoking an Issuing CA Certificate. QuoVadis updates the CRL for end-user Certificates at least every 12.5 hours and the date of the nextUpdate field will not be more than 72.5 hours after the date in the thisUpdate field.

Before revoking an Issuing CA Certificate a last CRL is generated with a “nextUpdate” field value of "99991231235959Z”. The last CRL is available in accordance with Section 5.5.2. QuoVadis does not issue a last CRL until all Certificates in the scope of the CRL are either expired or revoked.

After the expiry date of an Issuing CA the most recent CRL will be published for at least 24 hours. QuoVadis does not use the ExpiredCertsOnCRL extension.

### 4.9.8. Maximum Latency For CRL

CRLs for Certificates issued to end entity Subscribers are posted automatically to the online Repository within a commercially reasonable time after generation, usually within 10 minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

### 4.9.9. On-Line Revocation/Status Checking Availability

In addition to CRLs, QuoVadis also provides certificate status information via OCSP in accordance with RFC 6960. The OCSP service is updated immediately when a Certificate is revoked. OSCP responses are valid for a maximum of 48.5 hours. Where applicable, the URL for the OCSP responder may be found within the Authority Information Access (AIA) extension of the Certificate.

Upon expiry of the Issuing CA, the associated OCSP Responder service is discontinued. For Qualified and PKIoverheid Certificates, QuoVadis uses the OCSP ArchiveCutoff extension. QuoVadis does not compute a last OCSP answer for issued Certificates with the nextUpdate field set to "999912312359592".

OCSP responses of QuoVadis are signed by either:

- the Private Key for the CA which issued the Certificate for which the status is requested; or
- the Private Key of an OCSP Signing Certificate for an OCSP responder designated by QuoVadis;

In the latter case, the OCSP-Signing Certificate is also provided with the extension id-pkix-ocsp-nocheck which is not marked as "critical" and has the value "NULL" (*see* RFC6960)

### 4.9.10. OCSP Checking Requirement

A Relying Party must confirm the validity of a Certificate in accordance with Section 4.9.6 prior to relying on the Certificate. The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

QuoVadis supports an OCSP capability using the GET method for Certificates. OCSP responders under QuoVadis’ direct control respond with an "unauthorised" status for Certificates that have not been issued. QuoVadis may monitor its OCSP responders for requests for non-issued Certificates as part of its security response procedures.

### 4.9.11. Other Forms Of Revocation Advertisements Available

Not applicable.

### 4.9.12. Special Requirements Related To Key Compromise

QuoVadis uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. Reports to QuoVadis of key compromise must include:

- Proof of key compromise in either of the following formats:
    - A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for DigiCert"; or
    - The private key itself
- If a CSR is provided, QuoVadis will only accept proof of key compromise, if one of the following algorithms are used to sign the CSR:
    - SHA256WithRSA
    - SHA384WithRSA
    - SHA512WithRSA
    - ECDSAWithSHA256
    - ECDSAWithSHA384
    - ECDSAWithSHA512
    - SHA256WithRSAPSS
    - SHA384WithRSAPSS
    - SHA512WithRSAPSS
    - PureEd25519
- A valid Mailbox Address so that you can receive confirmation of your problem report and associated certificate revocations

QuoVadis will select the CRLReason code "keyCompromise" (value 1) upon discovery of such reason or as required by an applicable CP/CPS. Should a CA Private Key become compromised, the CA and all Certificates issued by that CA shall be revoked. QuoVadis provides additional instructions and support for keyCompromise at https://www.quovadisglobal.com/certificate-revocation/ and other resources as indicated in Section 1.5.2.1 of this CP/CPS.

### 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

Certificate status information is available via CRL and OCSP responder. For publicly-trusted TLS certificates, revocation entries on a CRL or OCSP Response are not removed until after the expiration of the revoked Certificate. The serial number of a revoked Certificate remains on the CRL until one additional CRL is

published after the end of the Certificate's validity period, except for revoked Code Signing Certificates, which remain on the CRL for at least 10 years following the Certificate's validity period.

### 4.10.2. Service Availability

Certificate status services are available 24x7. QuoVadis operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

QuoVadis also maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

### 4.10.3. Optional Features

No stipulation.

## *4.11. END OF SUBSCRIPTION*

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

## *4.12. KEY ESCROW AND RECOVERY*

QuoVadis provides optional Private Key Escrow services for certain Certificate Profiles (*see* Appendix A, Section 10.1.2) under this CP/CPS. Private Key Escrow is only available if the Enterprise RA Administrator directs at the Account level. Private Key Escrow is prohibited for the following Certificate types:

- CA Certificates
- QV Advanced+ Certificates
- QV Qualified Certificates
- Any Certificate whose Private Key Usage is dedicated to Signing or Authentication
- TLS Certificates
- Codesigning Certificates

Private Key Escrow shall not be allowed when the nonRepudiation keyUsage is present in a Certificate as of version 4.32 of this CP/CPS.

### 4.12.1. Key Escrow And Recovery Policy And Practices

Issuing CAs shall not escrow CA Private Keys.

Issuing CAs may escrow Subscriber key management keys to provide key recovery services. Issuing CAs shall encrypt and store escrowed Private Keys with at least the level of security used to generate and deliver the Private Key. Issuing CAs shall protect Private Keys from unauthorized disclosure.

Enterprise customers utilizing key escrow services provided by QuoVadis may escrow keys within their infrastructure. Enterprise customers must notify subscribers when keys are escrowed.

Subscribers and other authorized entities may request recovery of an escrowed (decryption) Private Key. Keys are recovered at the request of the Subscriber, contracting entity or as required by law.

Entities escrowing Private Keys shall have personnel controls in place that prevent unauthorized access to Private Keys.

### 4.12.2. Session Key Encapsulation And Recovery Policy And Practices

Not applicable.

# 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Section of the CP/CPS provides a high level description of the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by QuoVadis to provide trustworthy and reliable CA operations. QuoVadis maintains a security program to:

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

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

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

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

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

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

## *5.1. PHYSICAL CONTROLS*

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

### 5.1.1. Site Location and Construction

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

### 5.1.2. Physical Access

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

### 5.1.3. Power And Air-Conditioning

Datacentres have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and generators provide redundant backup power.

### 5.1.4. Water Exposures

The cabinets housing QuoVadis' CA and TSA systems are designed to prevent and protect against water exposure.

### 5.1.5. Fire Prevention And Protection

QuoVadis datacentres are equipped with fire suppression mechanisms.

### 5.1.6. Media Storage

QuoVadis protects its media from accidental damage, environmental hazards, unauthorised physical access, and from obsolescence/deterioration during the period that records are required to be retained. Backup files are created on a daily basis. QuoVadis backup files are maintained at either within the QuoVadis service operations area or in a secure off-site storage area.

### 5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

### 5.1.8. Off-Site Backup

An off-site location is used for the storage and retention of backup software and data. The off-site storage is available to authorised personnel 24x7for 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

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

#### *5.2.1.1. CA Administrators*

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

#### *5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel*

The Registration Officer role is responsible for issuing and revoking Certificates.

#### *5.2.1.3. System Administrators/ System Engineers (Operator)*

The System Administrator/System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator/System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and recoverability.

#### *5.2.1.4. Internal Auditors*

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if QuoVadis, an Issuing CA, or RA is operating in accordance with this CP/CPS or approved registration procedures.

#### *5.2.1.5. RA Administrators*

RA Administrators are responsible for the RA certificate management systems.

#### *5.2.1.6. Security Officers*

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

### 5.2.2. Number Of Persons Required Per Task

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

### 5.2.3. Identification And Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure commensurate to their role and access privileges are configured using the "least privileges" principle for the role. All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

### 5.2.4. Roles Requiring Separation Of Duties

Trusted roles requiring a separation of duties include those performing:

- authorisation functions such as the verification of information in Certificate Requests and certain approvals of Certificate applications and revocation requests,
- backups, recording, and record keeping functions;
- audit, review, oversight, or reconciliation functions; and
- duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, QuoVadis specifically designates individuals to the trusted roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. QuoVadis systems identify and authenticate individuals acting in trusted roles and restrict an individual from assuming multiple roles at the same time.

## *5.3. PERSONNEL CONTROLS*

### 5.3.1. Qualifications, Experience, And Clearance Requirements

The PMA is responsible and accountable for QuoVadis PKI operations and ensures compliance with this CP/CPS. Prior to the engagement of any person in the Certificate management process, QuoVadis verifies the identity and trustworthiness of such person. QuoVadis determines that all individuals assigned to trusted roles perform their prospective job responsibilities competently and satisfactorily as required.

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

QuoVadis verifies the identity of each individual appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. QuoVadis' human resources department verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks may include a combination of the following as required; verification of individual identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background.

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this Section cannot be met by QuoVadis due to a prohibition or limitation in local law, QuoVadis utilises a substitute investigative technique permitted by law that provides

substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

### 5.3.3. Training Requirements

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

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

QuoVadis maintains records of who received training. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on relevant standards including the EV Guidelines, the TLS BR and the S/MIME BR prior to validating and approving the issuance of such Certificates.

### 5.3.4. Retraining Frequency And Requirements

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

### 5.3.5. Job Rotation Frequency And Sequence

Not applicable.

### 5.3.6. Sanctions For Unauthorised Actions

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

### 5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

### 5.3.8. Documentation Supplied To Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties.

## *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 Certificate, including all information generated and documentation received in connection with the Certificate Request. QuoVadis logs the following events:

- CA Certificate and key lifecycle management events;
  - Certificate requests, renewal, and re-key requests, and revocation;
  - Approval and rejection of Certificate Requests;
  - Cryptographic device lifecycle management events;
  - Generation of CRLs and OCSP entries; and
  - Certificate Profiles management.
- Subscriber Certificate lifecycle management events, including:
  - Certificate requests, renewal, and re-key requests, and revocation;
  - Verification activities;
  - Approval and rejection of Certificate Requests;
  - Issuance of Certificates; and
  - Generation of CRLs and OCSP entries.
- Security events, including
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - Installation, update and removal of software on a PKI System;
  - 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 record;
- Identity of the entity making the journal record; and
- Details of the record.

### 5.4.2. Frequency Of Processing Log

As required, generally within at least once every two months, a QuoVadis administrator reviews the logs generated by QuoVadis' systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (i) checks whether anyone has tampered with the log, (ii) scans for anomalies or specific conditions, including any evidence of malicious activity, and (iii) if necessary, prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries may include recommendations to DigiCert's operations management committee and are made available to auditors upon request. QuoVadis documents any actions taken as a result of a review.

### 5.4.3. Retention Period For Audit Log

Audit logs relating to the Certificate lifecycle are retained as archive records for a period no less than eleven (11) years for Swiss Qualified Certificates and for seven (7) years for all other Certificates starting from the destruction of the CA Private Key or revocation or expiration of the Certificate. Certain high volume system generated logs are retained for 24 months based on a risk assessment. QuoVadis makes the audit logs available to auditors, as defined in Section 8, available upon request.

### 5.4.4. Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI. Only certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction. All audit logs are protected in an encrypted format via a Key and Certificate generated especially for the purpose of protecting the logs.

### 5.4.5. Audit Log Backup Procedures

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

Backup procedures apply to the QuoVadis PKI and the Participants therein including the QuoVadis Root CAs, Issuing CAs, and RAs.

### 5.4.6. Audit Collection System

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

### 5.4.7. Notification To Event-Causing Subject

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

### 5.4.8. Vulnerability Assessment

QuoVadis performs monthly vulnerability scans on its PKI systems and infrastructure. Identified vulnerabilities are rated and addressed on the basis of the Common Vulnerability Scoring System (CVSS).

QuoVadis' audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

QuoVadis performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorised access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. QuoVadis also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that QuoVadis has in place to control risks identified in risk assessments. QuoVadis' Internal Auditors review the security audit data checks for continuity.

Based on the risk assessment, QuoVadis develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the Certificate data and management processes.

## *5.5. RECORDS ARCHIVAL*

### 5.5.1. Types Of Records Archived

QuoVadis archives records related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems, including event records and documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

QuoVadis archives records relating to:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1)
- Subscriber Certificate lifecycle management event records (as set forth in Section; and
- Security event records (as set forth in Section 5.4.1)

QuoVadis retains the following information in its archives (as such information pertains to QuoVadis' CA / TSA operations):

i) Accreditations of QuoVadis;

ii) CP/CPS versions;

iii) Contractual obligations and other agreements concerning the operation of the CA/TSA;

iv) System and equipment configurations, modifications, and updates;

v) Rejection or acceptance of a Certificate request;

vi) Certificate issuance, rekey, renewal, and revocation requests;

vii) Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes;

viii) Any documentation related to the receipt or acceptance of a Certificate or token;

ix) Subscriber Agreements;

x) Issued Certificates;

xi) A record of Certificate re-keys;

xii) Data or applications necessary to verify an archive's contents;

xiii) Compliance auditor reports;

xiv) Changes to QuoVadis audit parameters;

xv) Any attempt to delete or modify audit logs;

xvi) CA Key generation and destruction;

xvii) Access to Private Keys for key recovery purposes;

xviii) Changes to trusted Public Keys;

xix) Export of Private Keys;

xx) Approval or rejection of a revocation request;

xxi) Appointment of an individual to a trusted role;

xxii) Destruction of a cryptographic module;

xxiii) Certificate compromise notifications;

xxiv) Remedial action taken as a result of violations of physical security; and

xxv) Violations of the CP/CPS.

### 5.5.2. Retention Period For Archive

Audit logs relating to the Certificate lifecycle are retained as archive records for a period no less than eleven (11) years for Swiss Qualified Certificates and for seven (7) years for all other Certificates. Detailed system generated logs are retained for 24 months based on a risk assessment.

### 5.5.3. Protection Of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorised modification, substitution, or destruction. Archives are not released except as allowed by the PMA or as required by law. QuoVadis maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If QuoVadis needs to transfer any media to a different archive site or equipment, QuoVadis will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

### 5.5.4. Archive Backup Procedures

On at least an annual basis, QuoVadis creates an archive of the data listed in Section 5.5.1. Each archive is stored separately and available for integrity verification at a later date. QuoVadis stores the archive in a secure location for the duration of the set retention period.

### 5.5.5. Requirements For Time-Stamping Of Records

QuoVadis supports time stamping 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 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

Access to archives is granted only to persons in Trusted Roles and based on least privilege. 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*

### 5.7.1. Incident and Compromise Handling Procedures

QuoVadis maintains internal incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. These procedures include notification to Application Software Vendors, Subscribers, and Relying Parties as appropriate in the event of a disaster, security compromise, or business failure. QuoVadis reviews, tests, and updates its incident response plans and procedures on a periodic basis.

### 5.7.2. Computing Resources, Software, and/or Data Are Corrupted

QuoVadis makes regular system backups weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If QuoVadis discovers that any of its computing resources, software, or data operations have been compromised, QuoVadis assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If QuoVadis determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, QuoVadis suspends such operation until it determines that the risk is mitigated.

### 5.7.3. Entity Private Key Compromise Procedures

If QuoVadis suspects that one of its CA Private Keys has been compromised, the PMA will convene a response team to assess the incident and take appropriate action. QuoVadis will meet the requirements of Section 1.1 by following incident response plans whose steps generally include the following:

i) Collect information related to the incident;

ii) Determine the degree and scope of compromise; and report on the course of action that should be taken to correct the problem and prevent reoccurrence;

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

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

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

### 5.7.4. Business Continuity Capabilities After a Disaster

To maintain the integrity of its services, QuoVadis implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving QuoVadis' primary facility and that QuoVadis be capable of maintaining other services or resuming them as quickly as possible following a disaster. QuoVadis periodically reviews, tests, and updates the BCMP and supporting procedures.

## *5.8. CA AND/OR RA TERMINATION*

Unless otherwise addressed in an applicable agreement between QuoVadis and a counterparty, before terminating its CA or RA activities, QuoVadis may:

i) Notify relevant Government and Certification bodies under applicable laws and related regulations;

ii) Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors and by posting such information on QuoVadis' web site; and

iii) Transfer all responsibilities to a qualified successor entity.

Unless otherwise addressed in an applicable agreement between QuoVadis and a counterparty, if a qualified successor entity does not exist, QuoVadis may:

i) Transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;

ii) Revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;

iii) Destroy all Private Keys; and

iv) make other necessary arrangements that are in accordance with this CP/CPS.

| | |
|---|---|
| | For Qualified Certificates, a notice of termination of the Issuing CA must be communicated in accordance with pre-established procedures to SAS, the body responsible for accrediting the Certificate Service Provider. |
| | For EU Qualified Certificates, QuoVadis has implemented procedures to be followed in the event of termination of the service provision. These procedures provide for the transfer of relevant records to a regulatory body and the continuation of revocation status in the event of termination. QuoVadis also has formally documented complaint and dispute resolution procedures. |

QuoVadis has made arrangements to cover the costs associated with fulfilling these requirements in case QuoVadis becomes bankrupt or is unable to cover the costs. Any requirements of this Section that are varied by contract apply only the contracting parties.

# 6. TECHNICAL SECURITY CONTROLS

## *6.1. KEY PAIR GENERATION AND INSTALLATION*

### 6.1.1. Key Pair Generation

QuoVadis CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony in the environments described in Section 5.1 and logged in accordance with Section 5.4. The cryptographic hardware is evaluated to FIPS 140-2 Level 3 and/or Common Criteria EAL 4 or higher. Hardware Security Modules (HSM) are always stored in a physically secure environment and are subject to security controls throughout their lifecycle. Activation of the hardware requires the use of two-factor authentication tokens.

QuoVadis creates auditable evidence during the key generation process to prove that the CP/CPS was followed and role separation was enforced during the key generation process. QuoVadis requires that an external auditor witness the generation of or review a recording of any CA keys to be used as publicly-trusted Root Certificates. For other CA Key Pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Subscribers must generate their Key Pair in a manner that is appropriate for the Certificate type.

For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.

For Swiss Qualified Certificates of type QCP-n-qscd, and for Swiss Regulated Certificates, the Subscriber Private Keys are generated and stored on a QSCD.

In the case that a QSCD used by QuoVadis for QCP-n-qscd or QCP-l-qscd loses its certification status, non-expired Certificates using the affected QCSD will be revoked. In some cases, a QTSP generates and manages Private Keys on behalf of the Subscriber. This is signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies. *See also* Section 10.1.1.

For Adobe Acrobat Trust List (AATL) Certificates, Subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 3.

QuoVadis never creates key pairs for publicly-trusted TLS Certificates and will not accept a Certificate Request using a Key Pair previously generated by DigiCert or QuoVadis.

For publicly-trusted TLS Certificates, QuoVadis rejects a Certificate Request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 of the TLS BR or S/MIME BR (as applicable) or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

### 6.1.2. Private Key Delivery To Subscriber

Where QuoVadis generates Private Keys on behalf of the Subscriber, they are provided in a secure manner via the QuoVadis Portal (for example for S/MIME Certificates) or Digital Signature platform. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

- Except where escrow/backup services are authorised and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery;
- The key generator must protect the Private Key from activation, compromise, or modification during the delivery process;
- The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate; and
- The key generator delivers the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers securely.

| | |
|---|---|
| | For some EU Qualified and Swiss Qualified/Regulated Certificates, QuoVadis may generate and manage Private Keys on behalf of the Subscriber. Where the policy requires the use of a QSCD then the signatures shall only be created by the QSCD.<br><br>In the case of natural persons, the Subscribers' Private Key is maintained and used under their sole control and used only for Electronic Signatures. In the case of legal persons, the Private Key is maintained and used under their control and used only for Electronic Seals. |

If QuoVadis or an Enterprise RA becomes aware that a Subscriber's Private Key has been communicated to a person or organisation not authorised by the Subscriber, then QuoVadis will revoke all Certificates associated with that Private Key.

Electronic Signature Subscribers are solely responsible for the generation of the Private Keys used in their Certificate Requests.

### 6.1.3. Public Key Delivery To Certificate Issuer

Subscribers generate Key Pairs and deliver Public Keys to the Issuing CA in a secure and trustworthy manner, such as submitting a CSR message to a QuoVadis Portal.

### 6.1.4. CA Public Key To Relying Parties

QuoVadis' Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root stores, and/or as roots signed by other CAs. All Accreditation Authorities supporting QuoVadis Certificates and all Application Software Vendors are permitted to redistribute QuoVadis CA Certificates.

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

### 6.1.5. Key Sizes

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

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

Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm if it is compliant with all applicable programs listed in Section 1.1. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

QuoVadis requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms. QuoVadis may require higher bit keys in its sole discretion.

Any Root Certificates participating in the AATL program issued after July 1, 2017 must be at least 3072-bit for RSA and 256-bit for ECDSA.

QuoVadis and Subscribers may fulfill transmission security requirements using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

### 6.1.6. Public Key Parameters Generation And Quality Checking

QuoVadis uses cryptographic modules that conform to FIPS 186-2 and provide random value generation and on-board generation of Public Keys and a wide range of ECC curves.

### 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;

iii) Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

iv) Certificates for OCSP Response verification.

Subscriber Certificates assert key usages based on the intended application of the Key Pair and cannot include anyExtendedKeyUsage. Key usage bits and extended key usages are specified in Appendix A.

An Issuing CA's Private Keys may be used for Certificate signing and CRL and OCSP response signing and shall not be used for any other purpose.

## *6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS*

All Participants in the QuoVadis PKI are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this QuoVadis CP/CPS. Without limitation to the generality of the foregoing, all Participants in the QuoVadis PKI must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised use of their Private Key (to include password, Token or other activation data used to control access to the Private Key); and (ii) exercise sole and complete control and use of the Private Key that corresponds to their Public Key.

### 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 and/or Common Criteria EAL 4 security standards in both the generation and the maintenance in all Root and Issuing CA Private Keys.

| | |
|---|---|
| | For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.<br><br>For Swiss Qualified Certificates of type QCP-n-qscd, and Swiss Regulated Certificates, the Subscriber Private Keys are generated and stored on a QSCD.<br><br>In some cases, QuoVadis generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies. *See also* Section 10.1.1. |

QuoVadis must verify that QSCDs are certified as a QSCD in accordance requirements laid down in Annex II of the eIDAS Regulation. QuoVadis must monitor this certification status and take appropriate measures if the certification status of a QSCD changes. The QSCD certification status and evidence of the QuoVadis monitoring are in scope of the external eIDAS/ETSI conformity assessments.

Effective November 15, 2022 for Code Signing Certificates, Subscribers must generate and protect Private Keys:

- using a cryptographic module certified to FIPS 140-2 Level 2 or Common Criteria EAL 4+; or
- using cloud-based generation and protection solution as defined in Section 16.3.1 of the Code Signing Baseline Requirements; or
- using signing service as defined in Section 16.2 of the Code Signing Baseline Requirements.

### 6.2.2. Private Key (N of M) Multi-Person Control

QuoVadis' authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. Backups of CA Private Keys are securely stored and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

### 6.2.3. Private Key Escrow

QuoVadis does not escrow its CA signature keys. QuoVadis may provide escrow services for end entity Subscriber Certificates in order to provide key recovery as described in Section 4.12.1.

### 6.2.4. Private Key Backup

QuoVadis CA Private Keys are generated and operated inside cryptographic modules which have been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. QuoVadis' CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process.

QuoVadis may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

### 6.2.5. Private Key Archive

QuoVadis does not archive CA Certificate Private Keys.

### 6.2.6. Private Key Transfer Into Or From A Cryptographic Module

All CA keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, QuoVadis encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access. If QuoVadis becomes aware that an Issuing CA's Private Key has been communicated to an unauthorised person or an organisation not affiliated with the Issuing CA, then QuoVadis will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If QuoVadis pre-generates Private Keys and transfers them into a hardware token, for example transferring generated end-entity Subscriber Private Keys into a smart card, it will securely transfer such Private Keys into the token to the extent necessary to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such Private Keys.

### 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. Root CA Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

### 6.2.8. Method Of Activating Private Key

QuoVadis' Private Keys are activated according to the specifications of the HSM manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or equivalent authentication method to prevent unauthorised access or use of the Subscriber Private Key. When deactivated, Private Keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys.

### 6.2.9. Method Of Deactivating Private Key

QuoVadis' Private Keys are deactivated via manual and passive logout procedures on the applicable HSM device when not in use. QuoVadis never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

### 6.2.10. Method Of Destroying Private Key

QuoVadis personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

QuoVadis may destroy a Private Key by deleting it from all known storage partitions. QuoVadis also zeroises the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitialises the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, QuoVadis will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key. 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 and/or Common Criteria EAL 4 security standards or higher.

| | |
|---|---|
| | For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.<br><br>For Swiss Qualified Certificates of type QCP-n-qscd, and Swiss Regulated Certificates, the Subscriber Private Keys are generated and stored on a QSCD.<br><br>In some cases, QuoVadis generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies. *See also* Section 10.1.1. |

## *6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT*

### 6.3.1. Public Key Archival

QuoVadis archives copies of Public Keys in accordance with section 5.5.

### 6.3.2. Certificate Operational Periods And Key Pair Usage Periods

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

| **Type** | **Certificate Term** |
|---|---|
| Publicly-trusted Root CAs | 30 years |
| Publicly-trusted Issuing CAs | 15 years |

| Type | Certificate Term |
|---|---|
| Qualified Certificates for Electronic Signature and Electronic Seal | 12 to 36 months |
| TLS Certificates including Qualified Web Authentication Certificates (QEVCP-w) | 398 days |
| S/MIME Certificates | 1185 days |
| Code Signing Certificates | 39 months |

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day. For the purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximum requirements listed in Section 1.1 as applicable.

Relying Parties may still validate signatures generated with these keys after expiration of the Certificate.

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

## *6.4. ACTIVATION DATA*

### 6.4.1. Activation Data Generation And Installation

QuoVadis activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer meeting the requirements of FIPS 140-2 Level 3 and/or Common Criteria EAL 4. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CP/CPS. QuoVadis will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

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

### 6.4.2. Activation Data Protection

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

### 6.4.3. Other Aspects Of Activation Data

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

## *6.5. COMPUTER SECURITY CONTROLS*

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

### 6.5.1. Specific Computer Security Technical Requirements

QuoVadis secures its CA systems and authenticates and protects communications between its systems and trusted roles. QuoVadis' CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses. Inactivity log out timeframes are set and enforced through internal information security policies and procedures to ensure security.

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

RAs must logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs must require the use of passwords with a minimum character length and a combination of alphanumeric and special characters.

QuoVadis' CA systems are configured to:

i) authenticate the identity of users before permitting access to the system or applications;
ii) manage the privileges of users and limit users to their assigned roles;
iii) generate and archive audit records for all transactions;
iv) enforce domain integrity boundaries for security critical processes; and
v) support recovery from key or system failure.

All Certificate Status Servers:

i) authenticate the identity of users before permitting access to the system or applications;
ii) manage privileges to limit users to their assigned roles;
iii) enforce domain integrity boundaries for security critical processes; and
iv) support recovery from key or system failure.

QuoVadis enforces multi-factor authentication on any Portal account capable of directly causing Certificate issuance.

### 6.5.2. Computer Security Rating

No stipulation.

## *6.6. LIFE CYCLE TECHNICAL CONTROLS*

### 6.6.1. System Development Controls

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

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

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

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

### 6.6.2. Security Management Controls

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

### 6.6.3. Life Cycle Security Controls

No stipulation.

## *6.7. NETWORK SECURITY CONTROLS*

QuoVadis CA and RA functions are performed using networks secured in accordance with the standards documented in the CP/CPS to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and Digital Signatures for non-repudiation and authentication.

QuoVadis documents and controls the configuration of its systems, including any upgrades or modifications made. QuoVadis' CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). QuoVadis' customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses.

Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

QuoVadis performs vulnerability scans of its networks at least once a quarter, and penetration tests at least annually.

QuoVadis' security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. QuoVadis' network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

## *6.8. TIME-STAMPING*

*See* Section 5.5.5. In addition, QuoVadis provides Time-Stamp Authority (TSA) services for use with specific QuoVadis products such as Qualified Electronic Signatures or Code Signing Certificates. The QuoVadis Time-Stamp Policy/Practice Statement is structured in accordance with ETSI EN 319 421 and should be read in conjunction with this CP/CPS.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

QuoVadis uses the ITU X.509, version 3 standard to construct Certificates. QuoVadis adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. *See* Appendix A.

For publicly-trusted TLS Certificates, QuoVadis meets the technical requirements set forth in Sections 2.2, 6.1.5, and 6.1.6 of the TLS BR or S/MIME BR (as applicable) and this CP/CPS.

QuoVadis generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

## *7.1. CERTIFICATE PROFILE*

The table below describes the basic fields that may be included in QuoVadis Certificates. Refer to APPENDIX A for additional Certificate contents that are specific to the individual Certificate Profiles.

### 7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

### 7.1.2. Certificate Extensions

The extensions defined for X.509 v3 Certificates provide methods for associating additional attributes with users or Public Keys and for managing relationships between CAs. *See* Appendix A.

For Root CA, Subordinate CA, and Subscriber Certificates used for publicly-trusted Certificates, QuoVadis abides by the relevant Baseline Requirements and configures the Certificate extensions to those requirements.

Subordinate CA Certificates created after January 1, 2019 for publicly-trusted Certificates, with the exception of cross-certificates that share a private key with a corresponding Root Certificate, will contain an EKU extension, and cannot include the anyExtendedKeyUsage KeyPurposeId. QuoVadis no longer includes both the id-kp- serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

For TLS Certificates, the subjectAltName extension is populated in accordance with RFC 5280 with the authenticated value in the Common Name field of the subject DN (domain name or public iPAddress). The SubjectAltName extension may contain additional authenticated domain names or public iPAddresses. The name forms and extensions will abide by Section 7.1.4 of this CP/CPS and the TLS BR.

For internationalised domain names, the Common Name is represented as a puny-code value and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

For S/MIME Certificates, the subjectAltName extension must include contain at least one GeneralName entry Rfc822Name and/or an otherName of type id-on-SmtpUTF8Mailbox, encoded in accordance with RFC 8398. All Mailbox Addresses in the Subject or SAN entries of type dirName are repeated as Rfc822Name and/or an otherName of type id-on-SmtpUTF8Mailbox in the SAN.

QuoVadis' Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly-trusted certificates.

### 7.1.3. Algorithm Object Identifiers

QuoVadis Certificates are signed using one of the following algorithms or others as approved in accordance with Section 1.1:

| | |
|---|---|
| sha256WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11] |
| sha384WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12] |
| sha512WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13] |
| ecdsa-with-SHA256 | [iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 ] |
| ecdsa-with-SHA384 | [iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3] |
| id-RSASSA-PSS | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)] |

Issuing CAs shall not issue Certificates with SHA-1 as an algorithm.

RSASSA-PSS is not used for TLS Certificates and specifies the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.

QuoVadis and Subscribers may generate Key Pairs using the following:

| | |
|---|---|
| id-dsa | [iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1] |
| RsaEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1] |
| Dhpublicnumber | [iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1] |
| id-keyExchangeAlgorithm | [joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22] |
| id-ecPublicKey | [ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 ] |

Elliptic curve Public Keys submitted to QuoVadis for inclusion in end entity Certificates should be based on NIST "Suite B" curves.

As described in Section 1.2, QuoVadis uses the Key and hash algorithms specified in the relevant CA/Browser Forum Baseline Requirements. *See* also Appendix A.

### 7.1.4. Name Forms

Each Certificate includes a serial number that is unique to the Issuing CA. Optional subfields in the subject of an TLS Certificate must either contain information verified by QuoVadis or be left empty. TLS Server Certificates cannot contain metadata such as '.', '-' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable.

QuoVadis does not issue publicly-trusted TLS Certificates to a Reserved IP address or Internal Name, and does not issue publicly-trusted TLS or S/MIME Certificates with an OU attribute.

For CA Certificates, the commonName attribute is present contains an identifier that uniquely identifies the CA and distinguishes it from other CAs. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. Issuer DNs meet the requirements in the relevant CA/Browser Forum Baseline Requirements.

The contents of EV Certificates meet the requirements in Section 9 of the EV Guidelines.

The contents of S/MIME Certificates are validated according to Section 3 of this CP/CPS and the S/MIME Baseline Requirements. Enterprise RAs may include optional attributes in the certificate as specified in Section 7.1.4.2.5 of the S/MIME BR and are responsible for validating them in accordance with Section 3.

*See* also Appendix A.

### 7.1.5. Name Constraints

QuoVadis may use nameConstraints when appropriate. For publicly-trusted certificates, QuoVadis follows the requirements of Section 7.1.5 of the TLS BR and the S/MIME BR as relevant.

#### *7.1.5.1. Name-Constrained serverAuth CAs*

If the technically constrained Issuing CA Certificate includes the id-kp-serverAuth EKU, then it includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

i) For each dNSName in permittedSubtrees, QuoVadis confirms that the Applicant has registered the dNSName or has been authorised by the domain registrant to act on the registrant's behalf in line with the verification practices of TLS BR Section 3.2.2.4.

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

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

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

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

#### *7.1.5.2. Name-Constrained emailProtection CAs*

If the technically constrained Issuing CA includes the id-kp-emailProtection EKU, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to Section 7.1.5 of the S/MIME BR.

### 7.1.6. CP/CPS Object Identifier

An object identifier (OID) is a number unique that identifies an object or policy. Certificate Policy OIDs that incorporate this CP/CPS into different Certificate Profiles are listed in Appendix A.

### 7.1.7. Usage Of Policy Constraints Extension

Not applicable.

### 7.1.8. Policy Qualifiers Syntax And Semantics

QuoVadis Certificates may 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*

If present, this extension cannot be marked critical. This extension must be present for a Root CA or Issuing CA Certificate, including Cross Certificates. This extension may be present for Certificates not technically capable of causing issuance, subject to the requirement that the CRLReason cannot be certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate unless the reason is unspecified. QuoVadis may use the following reasonCode values from RFC 5280. When the CRLReason is not one of the following, then the reasonCode extension will not be provided:

- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)

In addition, QuoVadis administrators may assign the reasonCode for cACompromise (2) or privilegeWithdrawn (9).

For TLS Certificates issued on or after October 1, 2022 QuoVadis or a Subscriber are obligated to use the following CRLReasons appropriate for their revocation circumstances:

**keyCompromise**

The CRLReason keyCompromise will be used when one or more of the following occurs:

- QuoVadis obtains verifiable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise; or
- QuoVadis is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise; or
- There is clear evidence that the specific method used to generate the Private Key was flawed; or
- QuoVadis is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys); or
- the Subscriber requests that QuoVadis revoke the Certificate for this reason, with the scope of revocation being described below.

If anyone requesting revocation for keyCompromise has previously demonstrated or can currently demonstrate possession of the Private Key of the Certificate, then QuoVadis will revoke all instances of that key across all Subscribers.

If the Subscriber requests that QuoVadis revoke the Certificate for keyCompromise, and has not previously demonstrated and cannot currently demonstrate possession of the associated Private Key of that Certificate, QuoVadis may revoke all Certificates associated with that Subscriber that contain that public key.

When QuoVadis obtains verifiable evidence of Private Key compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, QuoVadis may update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, QuoVadis may update the revocation date in a CRL entry when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.

**privilegeWithdrawn**

The CRLReason privilegeWithdrawn is intended to be used when there has been a Subscriber-side infraction that has not resulted in keyCompromise, such as the Subscriber provided misleading information in their Certificate request or has not upheld their material obligations under the Subscriber agreement or Terms of Use.

Unless keyCompromise is being used, privilegeWithdrawn must be used when:

- QuoVadis obtains evidence that the Certificate was misused; or
- QuoVadis is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber agreement or Terms of Use; or
- QuoVadis is made aware that a wildcard Certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or
- QuoVadis is made aware of a material change in the information contained in the Certificate; or
- QuoVadis determines or is made aware that any of the information appearing in the Certificate is inaccurate; or
- QuoVadis is made aware that the original Certificate request was not authorised and that the Subscriber does not retroactively grant authorisation.

Otherwise, privilegeWithdrawn must not be used.

**cessationOfOperation**

The CRLReason cessationOfOperation is intended to be used when the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the domain name in the Certificate. This revocation reason is intended to be used in the following circumstances:

- the Subscriber no longer controls, or is no longer authorised to use, all of the domain names in the Certificate; or

- the Subscriber will no longer be using the Certificate because they are discontinuing their website; or
- 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).

Unless keyCompromise is being used, cessationOfOperation must be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- QuoVadis received verifiable evidence that the Subscriber no longer controls, or is no longer authorised to use, all of the domain names in the Certificate.

Otherwise, cessationOfOperation must not be used.

**affiliationChanged**

The CRLReason affiliationChanged is intended to be used to indicate that the Subject's name or other subject identity information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

Unless CRLReason is being used, affiliationChanged will be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- QuoVadis replaced the Certificate due to changes in the Certificate's subject information and the CA has not replaced the Certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Otherwise, affiliationChanged must not be used.

**superseded**

The CRLReason superseded is intended to be used to indicate when:

- the Subscriber has requested a new Certificate to replace an existing Certificate; or
- QuoVadis obtains reasonable evidence that the validation of domain authorisation or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon; or
- QuoVadis revoked the Certificate for compliance reasons such as the Certificate does not comply with the QuoVadis CP, this CPS, the relevant CA/Browser Forum Baseline Requirements, or the Mozilla Root Store Policy.

Unless the keyCompromise is being used, superseded must be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- QuoVadis revoked the Certificate due to domain authorisation or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, superseded must not be used.

### 7.2.1. Version Number

QuoVadis issues X.509 version 2 CRLs that may contain the following fields per requirements:

| Field | Value |
|---|---|
| Issuer Signature Algorithm | sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR<br>sha-384WithRSAEncryption [1 2 840 113549 1 1] OR<br>sha-512WithRSAEncryption [1 2 840 113549 1 1 13 ] OR |

| Field | Value |
|---|---|
| | ecdsa-with-sha256 [1 2 840 10045 4 3 2 ] OR<br>ecdsa-with-sha384 [1 2 840 10045 4 3 3] |
| Issuer Distinguished Name | QuoVadis Issuing CA name |
| thisUpdate | CRL issue date in UTC format |
| nextUpdate | Date when the next CRL will issue in UTC format. |
| Revoked Certificates List | List of revoked Certificates, including the serial number and revocation date |
| Issuer's Signature | [Signature] |

### 7.2.2. CRL And CRL Entry Extensions

QuoVadis CRLs may have the following extensions per RFC 5280 and other requirements as needed:

| Extension | Value |
|---|---|
| CRL Number | Never repeated monotonically increasing integer |
| Authority Key Identifier | Subject Key Identifier of the CRL issuer Certificate |
| Invalidity Date | Optional date in UTC format |
| Reason Code | Reason for revocation as described in Section 7.2 |
| Issuing Distribution Point | Configured per RFC 5280 requirements, if included. |

## *7.3. OCSP PROFILE*

### 7.3.1. OCSP Version Numbers

The QuoVadis OCSP Responders conform to version 1, as defined by RFC 6960. If an OCSP response is for a Root CA or Issuing CA, including Cross Certificates, and that Certificate has been revoked, the revocationReason field within the RevokedInfo of the CertStatus is present and asserted.

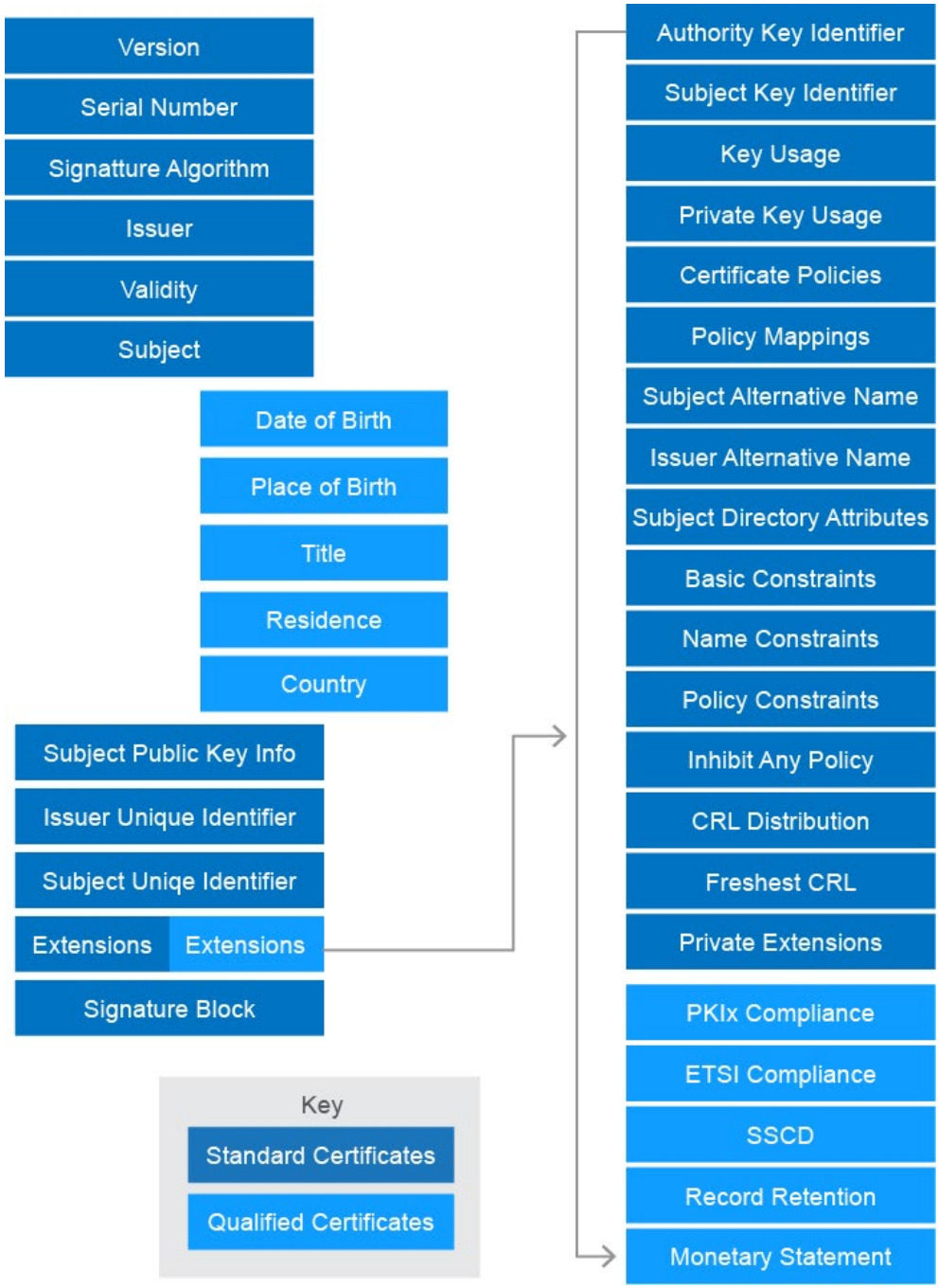
OCSP Responder Certificates have a maximum validity of 12 months.

### 7.3.2. OCSP Extensions

The singleExtensions of an OCSP response cannot contain the reasonCode (OID 2.5.29.21) CRL entry extension.

## *7.4. CERTIFICATE FIELDS AND ROOT CA CERTIFICATE HASHES*

### *7.4.1.* Certificate Fields



### 7.4.2. QuoVadis Root Certificate Hashes

Note that all QuoVadis CA Certificates and CRLs are available for download from the QuoVadis Repository at https://www.quovadisglobal.com/repository.

#### *7.4.2.1. QuoVadis Root CA 1 G3*

| Field | Certificate Profile |
|---|---|
| Serial Number | 78585F2EAD2C194BE3370735341328B596D46593 |
| SHA-256 Fingerprint | 8A866FD1B276B57E578E921C65828A2BED58E9F2F288054134B7F1F4BFC9CC74 |
| SPKI SHA-256 | 86A68F050034126A540D39DB2C5F917EF66A94FB9619FA1ECD827CEA46BA0CB0 |
| Valid To | Jan 12, 2042 |

#### *7.4.2.2. QuoVadis Root CA 2*

| Field | Certificate Profile |
|---|---|
| Serial Number | 0509 |
| SHA-256 Fingerprint | 85A0DD7DD720ADB7FF05F83D542B209DC7FF4528F7D677B18389FEA5E5C49E86 |
| SPKI SHA-256 | 8FD112C3C8370F147D5CCD3A7D865EB8DD540783BAC69FC60088E3743FF33378 |
| Valid To | Nov 24, 2031 |

#### *7.4.2.3. QuoVadis Root CA 2 G3*

| Field | Certificate Profile |
|---|---|
| Serial Number | 445734245B81899B35F2CEB82B3B5BA726F07528 |
| SHA-256 Fingerprint | 8FE4FB0AF93A4D0D67DB0BEBB23E37C71BF325DCBCDD240EA04DAF58B47E1840 |
| SPKI SHA-256 | 4A49EDBD2F8F8230BD5592B313573FE1C172A45FA98011CC1EDDBB36ADE3FCE5 |
| Valid To | Jan 12, 2042 |

#### *7.4.2.4. QuoVadis Root CA 3*

| Field | Certificate Profile |
|---|---|
| Serial Number | 05C6 |
| SHA-256 Fingerprint | 18F1FC7F205DF8ADDDEB7FE007DD57E3AF375A9C4D8D73546BF4F1FED1E18D35 |
| SPKI SHA-256 | 0C7ACAA710226720BBC940349EE2E6148652A89DBF406A232C895F6DC78EBB9A |
| Valid To | Nov 24, 2031 |

#### *7.4.2.5. QuoVadis Root CA 3 G3*

| Field | Certificate Profile |
|---|---|
| Serial Number | 2EF59B0228A7DB7AFFD5A3A9EEBD03A0CF126A1D |
| SHA-256 Fingerprint | 88EF81DE202EB018452E43F864725CEA5FBD1FC2D9D205730709C5D8B8690F46 |
| SPKI SHA-256 | F3438E23B3CE532522FACF307923F58FD18608E9BA7ADDC30E952B43C49616C3 |
| Valid To | Jan 12, 2042 |

## *7.5. CERTIFICATE TRANSPARENCY*

QuoVadis TLS Certificates MAY include Signed Certificate Timestamps (SCT) from independent CT 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 in this CP/CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for CAs as required by the Mozilla Root Store policy and other programs and standards listed in Section 1.1 and 1.6.3.

Publicly available audit reports provided by Conformance Assessment Bodies responsible for these audits will be published at https://www.quovadisglobal.com/accreditations. Compliance audits as carried out under these provisions may substitute for audits noted in this CP/CPS.

## *8.2. IDENTITY AND QUALIFICATIONS OF ASSESSOR*

WebTrust auditors must meet the requirements of Section 8.2 of the TLS BR, S/MIME BR, and Mozilla Root Store Policy as relevant. ETSI Conformance Assessment Bodies must meet the requirements of the relevant national accrediting authority. Auditors shall be experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies.

## *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*

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

Each audit scheme used by QuoVadis incorporates periodic monitoring and/or accountability procedures to ensure that audits continue to be conducted in accordance with the requirements of the scheme. Audits are conducted by a Qualified Auditor, as specified in Section 8.2.

## *8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY*

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to QuoVadis' services, then (i) the auditor will document the discrepancy, (ii) the auditor will promptly notify QuoVadis, and (iii) QuoVadis will develop a plan to cure the noncompliance. QuoVadis will submit the plan to the PMA for approval and to any third party that QuoVadis is legally obligated to satisfy. The PMA may require additional action if necessary to rectify any significant issues created by the

non-compliance, including requiring revocation of affected Certificates. QuoVadis is entitled to suspend and/or terminate services through revocation or other actions as deemed by the PMA to address the non-compliant Issuing CA.

| | |
|---|---|
| | For Qualified Certificates, the course of action and time frame for rectification of any deficiency as set by the relevant accrediting authority must be followed. |

## *8.6. COMMUNICATION OF AUDIT RESULTS*

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

## *8.7. SELF AUDITS*

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

# 9. OTHER BUSINESS AND LEGAL MATTERS

## *9.1. FEES*

### 9.1.1. Certificate Issuance Or Renewal Fees

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

### 9.1.2. Certificate Access Fees

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

### 9.1.3. Revocation Or Status Information Access Fees

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

### 9.1.4. Fees For Other Services

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

### 9.1.5. Refund Policy

QuoVadis or Issuing CAs under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements.

## *9.2. FINANCIAL RESPONSIBILITIES*

### 9.2.1. Insurance Coverage

QuoVadis maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

| | |
|---|---|
| | In accordance with ZertES, policy limits concerning Swiss Qualified Certificates are maintained in excess of CHF Two Million per occurrence and CHF Eight Million annual aggregate. |

### 9.2.2. Other Assets

No stipulation.

### 9.2.3. Insurance Or Warranty Coverage For End-Entities

No stipulation.

### 9.2.4. Fiduciary Relationships

QuoVadis is not the agent, fiduciary or other representative of any Subscriber and/or Relying Party and must not be represented by the Subscriber and/or Relying Party to be so. Subscribers and/or Relying Parties have no authority to bind QuoVadis by contract or otherwise, to any obligation.

Participation in the QuoVadis PKI does not make any participant an agent, fiduciary, trustee, or other representative of any entity, legal or otherwise. Nothing contained in this QuoVadis CP/CPS or in any corresponding Subscriber or Relying Party Agreement shall be deemed to constitute QuoVadis, QuoVadis PKI Participants or any of their agents, directors, employees, consultants, suppliers, contractors, partners or Counterparties a fiduciary, endorser, promoter, agent, partner, representative, or Counterparty of any entity, and the use of or reliance upon Certificates or other forms of participation within the QuoVadis PKI is to be construed accordingly.

## *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.

i) Private Keys;

ii) Activation data used to access Private Keys or to gain access to the CA system;

iii) Business continuity, incident response, contingency, and disaster recovery plans;

iv) Other security practices used to protect the confidentiality, integrity, or availability of information;

v) Information held by QuoVadis as private information in accordance with Section 9.4;

vi) Audit logs and archive records; and

vii) 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).

Any personal or corporate information held by Issuing CAs related to a Subscriber's application and the issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant Holder, unless required otherwise by law or to fulfil the requirements of this QuoVadis CP/CPS.

There is no requirement to place a copy of any Private Key with any backup/recovery or escrow service. Under contract between an Issuing CA and a Subscriber or the Subscriber's Nominating RA, a copy of an entity's encryption Keys may be escrowed by QuoVadis for possible retrieval of encrypted information upon the loss or corruption of the original encryption Keys.

### 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.

### 9.3.3. Responsibility To Protect Confidential Information

QuoVadis employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

## *9.4. PRIVACY OF PERSONAL INFORMATION*

### 9.4.1. Privacy Plan

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

### 9.4.2. Information Treated As Private

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

### 9.4.3. Information Deemed Not Private

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

### 9.4.4. Responsibility To Protect Private Information

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

### 9.4.5. Notice And Consent To Use Private Information

In the course of accepting a Certificate, individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of QuoVadis, 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 appear in publicly accessible directories and be communicated to others.

### 9.4.6. Disclosure Pursuant To Judicial Or Administrative Process

If required by a legitimate and lawful judicial order or regulation that complies with requirements of this CP/CPS, QuoVadis may disclose private information without notice.

### 9.4.7. Other Information Disclosure Circumstances

No stipulation.

## *9.5. INTELLECTUAL PROPERTY RIGHTS*

QuoVadis owns the intellectual property rights in QuoVadis' services, including the Certificates, trademarks and the Proprietary Marks used in providing the services, and this CP/CPS.

For the avoidance of doubt, external documents or electronic records signed or protected using QuoVadis Certificates are not considered to be QuoVadis documents for the purposes of this Section, nor is QuoVadis responsible for the content of those documents or records.

### 9.5.1. Property Rights In Certificates And Revocation Information

QuoVadis retains all intellectual property rights in and to the Certificates and revocation information that it issues. QuoVadis and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. QuoVadis, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

### 9.5.2. Property Rights In The CP/CPS

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

### 9.5.3. Property Rights In Names

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

### 9.5.4. Property Rights In Keys And Key Material

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

### 9.5.5. Violation Of Property Rights

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

## *9.6. REPRESENTATIONS AND WARRANTIES*

### 9.6.1. CA Representations And Warranties

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

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

QuoVadis discharges its obligations by:

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

QuoVadis hereby warrants (i) it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue (ii) Certificates shall be revoked if QuoVadis believes or is notified that the contents of the Certificate are no longer accurate, or that the Private 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.

QuoVadis provides test certificates for all types of Certificates.

### 9.6.2. RA Representations And Warranties

RAs represent and warrant that:

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

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

iii) Reasonable steps are taken to verify that the information contained in any Certificate is accurate at the time of issue;

iv) Translations performed by the RA are an accurate translation of the original information;

v) All Certificates requested by the RA meet the requirements of this CP/CPS and RA Agreement; and

vi) The RA will request that Certificates be revoked by QuoVadis if they believe or are 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' RA Agreement may contain additional representations. Subscriber Agreements may include additional representations and warranties.

### 9.6.3. Subscriber Representations And Warranties

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorised. Subscribers are required to notify QuoVadis and any applicable RA if a change occurs that could affect the status of the Certificate.

QuoVadis requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this Section for the benefit of QuoVadis and all Relying Parties and Application Software Vendors. This make take the form of either:

i) The Applicant's agreement to the Subscriber Agreement with QuoVadis; or

ii) The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to QuoVadis, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

i) Securely generate its Private Keys and protect its Private Keys from compromise, and exercise sole and complete control and use of its Private Keys;

ii) Provide accurate and complete information when communicating with QuoVadis, and to respond to QuoVadis' instructions concerning Key Compromise or Certificate misuse;

iii) Confirm the accuracy of the certificate data prior to installing or using the Certificate;

iv) For Qualified Certificates (a) if the policy requires the use of a QSCD, Electronic Signatures must only be created by a QSCD, (b) in the case of natural persons, the Private Key should only be used for Electronic Signatures, and (c) in the case of legal persons, the Private Key must be maintained and used under the control of the Subscriber and it should only be used for Electronic Seals.

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

vi) For Remote Identity Verification, use the identity proofing software distributed by QuoVadis. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;

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

viii) Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, including only installing TLS Server Certificates on servers accessible at the Domain listed in the Certificate and not using Code Signing Certificates to sign malicious code or any code that is downloaded without a user's consent; and

ix) Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that QuoVadis notifies the Subscriber that the QuoVadis PKI has been compromised.

Subscriber Agreements may include additional representations and warranties.

### 9.6.4. Relying Parties Representations And Warranties

Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. A Relying Party must exercise Reasonable Reliance as set out in this Section.

i) Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by QuoVadis related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available).

| | |
|---|---|
| | To be relied upon as an EU Qualified Certificate, the CA/trust anchor for the validation of the Certificate shall be as identified in a service digital identifier of an EU Trusted List entry with service type identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC" for a QTSP. ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted Lists. ETSI TS 119 172-4 describes how to validate a digital signature to determine whether it can be considered as an EU Qualified electronic signature or seal. |

ii) Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by QuoVadis.

iii) Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties reliance will be deemed reasonable if:

- the attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
- the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
- the Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
- the Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- the Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Certificate being relied upon;
- the Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
- the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
- the identity of the Subscriber is displayed correctly by utilising trusted application software; and
- any alterations arising from security changes are identified by utilising trusted application software.

If the circumstances indicate a need for additional assurances, it is Relying Parties' responsibility to obtain such assurances. A Relying Party shall make no assumptions about information that does not appear in a Certificate. All obligations within this Section relate to Reasonable Reliance on the validity of a Digital Signature, not the accuracy of the underlying electronic record. Relying Party Agreements may include additional representations and warranties.

### 9.6.5. Representations And Warranties Of Other Participants

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

## *9.7. DISCLAIMERS OF WARRANTIES*

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

## *9.8. LIABILITY AND LIMITATIONS OF LIABILITY*

This Section 9.8 does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CP/CPS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) QUOVADIS AND ITS AFFILIATES, SUBSIDIARIES,

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

| | |
|---|---|
| | For Swiss Qualified Certificates, QuoVadis liability is in accordance with Articles 17, 18, 19 of ZertES. |
| | For EU Qualified Certificates, QuoVadis liability is in accordance with Extract 37 and Article 13 of the eIDAS Regulation. |

## *9.9. INDEMNITIES*

### 9.9.1. Indemnification By QuoVadis

To the extent permitted by applicable law, QuoVadis shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an Certificate issued by QuoVadis, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (i) a valid and trustworthy Certificate as not valid or trustworthy or (ii) displaying as trustworthy (a) an Certificate that has expired or (b) a revoked Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

### 9.9.2. Indemnification By Subscribers

To the extent permitted by law, each Subscriber shall indemnify QuoVadis, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorised use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key. The applicable Subscriber Agreement may include additional indemnity obligations.

### 9.9.3. Indemnification By Relying Parties

To the extent permitted by law, each Relying Party shall indemnify QuoVadis, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

## *9.10. TERM AND TERMINATION*

### 9.10.1. Term

This CP/CPS and any amendments to this CP/CPS are effective when published in the QuoVadis Repository and remain in effect until replaced with a newer version.

### 9.10.2. Termination

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

### 9.10.3. Effect Of Termination And Survival

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

## *9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS*

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

Notices to Application Software Vendors are sent out in accordance with the respective requirements.

## *9.12. AMENDMENTS*

### 9.12.1. Procedure For Amendment

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

### 9.12.2. Notification Mechanism And Period

QuoVadis posts CP/CPS revisions to the Repository (https://www.quovadisglobal.com/repository). The QuoVadis PMA is responsible for determining what constitutes a material change of the CP/CPS. For routine modifications, QuoVadis does not guarantee or set a notice-and-comment period and may make changes to this CP/CPS without notice and without changing the version number. When the QuoVadis PMA determines a CP/CPS change may have a significant impact on Subscribers or Relying Parties, due notice of seven (7) days will be provided in the Repository. Subscribers whose Certificates remain valid at the effective date of the CP/CPS change shall be deemed to have accepted the modification.

### 9.12.3. Circumstances Under Which Object Identifiers Must Be Changed

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

## *9.13. DISPUTE RESOLUTION PROVISIONS*

For general complaints Subscribers and Subjects can send an email to qv.complaints@digicert.com.

For dispute resolution, to the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Participant shall notify QuoVadis, and

any other party to the dispute for the purpose of seeking business resolution. Both Participant and QuoVadis shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this CP/CPS and other relevant agreements.

i) Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.

ii) Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

| | |
|---|---|
| | For Swiss Qualified Certificates, such arbitration shall, unless agreed otherwise between the parties, take place in Switzerland. |
| | For Qualified Certificates issued in accordance with eIDAS, arbitration for disputes related to financial or commercial matters will be dealt with in the country of the relevant QuoVadis entity named in the contract with the client. Arbitration for Certificate-related disputes will be dealt with in the country named in relevant QuoVadis Issuing CA Certificate. |

## *9.14. GOVERNING LAW*

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-Section (i) above, will each depend on where Customer is domiciled as set forth in the table below; provided, for clarity, that rights and obligations arising from other applicable local laws continue to be governed by such laws, including with respect to EU Regulation 910/2014 (i.e., eIDAS), the General Data Protection Regulation (GDPR), and trade compliance laws.

In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

| Customer is Domiciled in or the Services are: | Governing Law is laws of: | Court or arbitration body with exclusive jurisdiction: |
|---|---|---|
| The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below | Utah state law and United States federal law | State and Federal courts located in Salt Lake County, Utah |
| Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa | England | International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in the below city corresponding to the QuoVadis contracting entity listed in the Order Form.<br><br>For QV CH: Zurich<br>For QV NL: Amsterdam<br>For QV DE: Munich<br>For QV BE/DigiCert Europe: Brussels<br>For QV UK: London |
| Japan | Japan | International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo |
| Australia or New Zealand | Australia | International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne |
| A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand | Singapore | International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore |

## *9.15. COMPLIANCE WITH APPLICABLE LAW*

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

## *9.16. MISCELLANEOUS PROVISIONS*

### 9.16.1. Entire Agreement

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

### 9.16.2. Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of QuoVadis. Unless specified otherwise in a contact with a party, QuoVadis does not provide notice of assignment.

### 9.16.3. Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

### 9.16.4. Enforcement (Attorneys' Fees And Waiver Of Rights)

QuoVadis may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. QuoVadis' failure to enforce a provision of this CP/CPS does not waive QuoVadis' right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by QuoVadis.

### 9.16.5. Force Majeure

QuoVadis is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond QuoVadis' reasonable control. The operation of the Internet is beyond QuoVadis' reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting QuoVadis. See also Section 9.8.3 (Excluded Liability) above.

## *9.17. OTHER PROVISIONS*

No stipulation.

# 10. APPENDIX A

## *10.1. CERTIFICATE PROFILES*

Within the QuoVadis PKI an Issuing CA can only issue Certificates with approved Certificate Profiles. All Certificate Profiles within the QuoVadis PKI are detailed below.

Procedures for Subscriber registration as well as descriptions of fields are described below for each type of Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described in this CP/CPS may be drawn up under contract for individual Subscribers.

### 10.1.1. QuoVadis Certificate Class

| Certificate Class | Description | Policy OID | Assurance Level | Requires token? |
|---|---|---|---|---|
| QV Standard | Based on the ETSI Lightweight Certificate Policy (LCP), which has the policy identifier OID 0.4.0.2042.1.3 | QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.100 (optional, may also use S/MIME BR OIDs)<br>ETSI policy identifier OID: 0.4.0.2042.1.3 (optional) | Low | Optional |
| QV Advanced | Based on the ETSI Normalised Certificate Policy (NCP), which has the OID 0.4.0.2042.1.1. Features face-to-face (or equivalent) authentication of holder identity and organisational affiliation (if included). | QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.200<br>ETSI policy identifier OID: 0.4.0.2042.1.1 (optional) | Medium | Optional |
| QV Advanced + | Similar to "QV Advanced" issued on an SSCD. Based on the ETSI Normalised Certificate Policy requiring an SSCD (NCP+), which has the OID 0.4.0.2042.1.2<br>Includes Swiss Regulated Certificates. | QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300<br>ETSI policy identifier OID: 0.4.0.2042.1.2 (optional) | High | Yes<br>Adobe AATL Approved |
| QV Qualified | QuoVadis Qualified Certificate on a QSCD | QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.400<br>ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd)<br>0.4.0.194112.1.3 (QCP-l-qscd) | High | Yes<br>Adobe AATL Approved |
| | QuoVadis Qualified Certificate on a QSCD, where the device is managed by a QTSP. | QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.410 | High | Yes |

| Certificate Class | Description | Policy OID | Assurance Level | Requires token? |
|---|---|---|---|---|
| | Relevant to the Policy in ETSI EN 319 411-2 for:<br>EU Qualified Certificates issued to a natural person (QCP-n-qscd), with the OID 0.4.0.194112.1.2<br>EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the OID 0.4.0.194112.1.3 | ETSI policy identifier OIDs:<br>0.4.0.194112.1.2 (QCP-n-qscd)<br>0.4.0.194112.1.3 (QCP-l-qscd) | | Adobe AATL Approved |
| | QuoVadis Qualified Certificate not on a QSCD.<br>Relevant to the Policy in ETSI EN 319 411-2 for:<br>EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0<br>EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1 | QuoVadis Certificate Class OID:<br>1.3.6.1.4.1.8024.1.450<br>ETSI policy identifier OIDs:<br>0.4.0.194112.1.0 (QCP-n)<br>0.4.0.194112.1.1 (QCP-l) | High | No |
| | QuoVadis Qualified Certificate not on a QSCD, where the device is managed by a QTSP.<br>Relevant to the Policy in ETSI EN 319 411-2 for:<br>EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0<br>EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1 | QuoVadis Certificate Class OID:<br>1.3.6.1.4.1.8024.1.460<br>ETSI policy identifier OIDs:<br>0.4.0.194112.1.0 (QCP-n)<br>0.4.0.194112.1.1 (QCP-l) | High | No |
| QV Closed Community | Used for reliance by members of the Issuer community only. Policies are defined in the CP/CPS of the Issuing CA. | 1.3.6.1.4.1.8024.1.500 | Medium | Optional |
| QV Device | Issued to devices, including Time-stamp Certificates. | 1.3.6.1.4.1.8024.1.600 | Medium | Optional |

### 10.1.2. Key Usage And Escrow

Different QuoVadis Certificate Profiles may be issued with different key usages, and be eligible for optional Key Escrow, according to the following table:

| **Certificate Type** | **Key Usage/ Extended Key Usage Options** | **Applicability to QuoVadis Certificate Classes** | | | |
|---|---|---|---|---|---|
| | | **QV Standard** | **QV Advanced** | **QV Advanced +** | **QV Qualified** |
| Signing and Encryption | **Key Usage**<br>digitalSignature<br>nonRepudiation<br>keyEncipherment<br>keyAgreement<br>**Extended Key Usage**<br>smartcardlogon<br>clientAuth<br>emailProtection<br>documentSigning<br>enrolmentAgent | Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL) | Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL) | Allowed (Escrow not permitted) | Not Allowed |
| Signing | **Key Usage**<br>digitalSignature<br>nonrepudiation<br>**Extended Key Usage**<br>smartcardlogon<br>clientAuth<br>emailProtection<br>documentSigning<br>enrolmentAgent | Allowed (Escrow not permitted) | Allowed (Escrow not permitted) | Allowed (Escrow not permitted) | Allowed (Escrow not permitted) |
| Encryption | **Key Usage**<br>keyEncipherment<br>keyAgreement<br>**Extended Key Usage**<br>emailProtection | Allowed (Escrow permitted) | Allowed (Escrow permitted) | Allowed (Escrow not permitted) | Not Allowed |
| Authentication | **Key Usage**<br>digitalSignature<br>**Extended Key Usage**<br>smartcardlogon<br>clientAuth<br>enrolmentAgent | Allowed (Escrow not permitted) | Allowed (Escrow not permitted) | Allowed (Escrow not permitted) | Not Allowed |

The Certificate Profiles that follow indicate the fields which are VARIABLE on initial registration by the Subscriber ("Holder Variable") and those which are FIXED by the Issuing CA either based on policy or by IETF Standard, applicable law, or regulation.

## *10.2. QV STANDARD*

| **Purpose** | | |
|---|---|---|
| Standard Certificates provide flexibility for a range of uses appropriate to their reliance value including S/MIME, electronic signatures, authentication, and encryption. | | |
| **Registration Process** | | |
| Validation procedures for QuoVadis Standard Certificates collect either direct evidence or an Attestation from an appropriate and authorised source of the identity (such as name and organisational affiliation) and other specific attributes of the Subject.<br><br>Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. Identity proofing may be conducted via enterprise records, physical presence; Remote Identity Verification (RIV1-4), reliance on electronic signature, or video verification. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory) (GN+SN or Pseudonym)<br>/GN (optional)<br>/SN (optional)<br><br>Pseudonym (optional)<br><br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory) | See definitions in Section 7.1.1.<br><br>Variable |
| SAN | /E<br>1.3.6.1.4.1.311.20.2.3 UPN | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.100 QV Standard Certificate (optional)<br>0.4.0.2042.1.3 ETSI LCP OID (optional)<br>2.23.140.1.5.1.1 S/MIME Mailbox-Legacy (optional)<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional) | Fixed |
| Key Usage (Critical) | digitalSignature (optional)<br>nonRepudiation<br>keyEncipherment (optional)<br>keyAgreement (optional) | Variable |
| Extended Key Usage | clientAuth<br>emailProtection<br>documentSigning<br>smartcardLogon<br>enrolmentAgent | Variable (at least one is present) |

## *10.3. QV ADVANCED*

| **Purpose** | | |
|---|---|---|
| QV Advanced Certificates provide reliable verification of the Subject's identity and may be used for a broad range of applications including Digital Signatures, encryption, and authentication. | | |
| **Registration Process** | | |
| Validation procedures for QV Advanced Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1.<br>Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on electronic signature. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br>= Legal Person (/O)<br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br>Pseudonym (optional for natural person)<br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory) | See definitions in Section 7.1.1<br>Variable |
| SAN | /E<br>1.3.6.1.4.1.311.20.2.3 UPN | **Variable** |
| Certificate Policies | 1.3.6.1.4.1.8024.1.200 QV Advanced Certificate<br>0.4.0.2042.1.1 ETSI NCP OID (optional)<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional) | Fixed |
| Key Usage (Critical) | digitalSignature (optional)<br>nonRepudiation<br>keyEncipherment (optional) | Variable |
| Extended Key Usage | clientAuth<br>emailProtection<br>documentSigning<br>smartcardLogon | Variable (at least one is present) |

## *10.4. QV ADVANCED +*

| **Purpose** | | |
|---|---|---|
| QuoVadis Advanced+ Certificates are used for the same purposes as QuoVadis Advanced Certificates, with the only difference being that they are issued on a Secure Cryptographic Device. The QuoVadis Advanced+ Certificate Class is trusted in the Adobe Approved Trust List (AATL). | | |
| **Registration Process** | | |
| QuoVadis Advanced+ Certificates are based on with the Normalised Certificate Policy (NCP+) described in ETSI EN 319 411-1.<br><br>Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification, or reliance onelectronic signature. AATL Certificates may use RIV1 or higher, ETSI Certificates may use RIV4 for NFC with RIV2 as a fallback option if NFC is not available.<br><br>QuoVadis Advanced+ Certificates must be issued on a Secure Cryptographic Device either held by the Subscriber or managed by QuoVadis and adhere to the following requirements:<br>• Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA or RA;<br>• User activation data is securely prepared and distributed separately from the Secure Cryptographic Device;<br>• If keys are generated under the Subscriber's control, they are generated within the Secure Cryptographic Device used for signing or decrypting;<br>• The Subscriber's Private Key can be maintained under the subject's sole control; and<br>• Only use the Subscriber's Private Key for signing or decrypting with the Secure Cryptographic Device. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br>= Legal Person (/O)<br><br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br><br>Pseudonym (optional for natural person)<br><br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory) | See definitions in Section 7.1.1<br><br>Variable |
| SAN | /E<br>1.3.6.1.4.1.311.20.2.3 UPN | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.300 QV Advanced+ Certificate<br>0.4.0.2042.1.2 ETSI NCP+ OID (optional)<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional) | Fixed |

| | | |
|---|---|---|
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | digitalSignature (optional)<br>nonRepudiation<br>keyEncipherment (optional) | Variable |
| Extended Key Usage | clientAuth<br>emailProtection<br>documentSigning<br>smartcardLogon | Variable (at least one is present) |

## *10.5. EIDAS QUALIFIED*

### 10.5.1. eIDAS Qualified Certificate issued to a Natural Person on a QSCD

| **Purpose** | | |
|---|---|---|
| The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation. These Certificates meet the relevant ETSI "Policy for EU Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd).<br><br>Swiss Qualified certificates issued under the Swiss Federal signature law (ZertES) also meet the ETSI policy QCP-n- qscd. These Swiss Qualified certificates are issued only to natural persons out of the "QuoVadis Swiss Regulated CAs" and have the notice text "qualified certificate" in the CertificatePolicies user notice.<br><br>The content of these Certificates meet the relevant requirements of:<br>• ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures<br>• ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons<br>• ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements | | |
| **Registration Process** | | |
| Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd). QuoVadis recommends that QCP-n-qcsd certificates are used only for electronic signatures.<br><br>Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. Only methods approved for eIDAS Qualified Certificates may be used. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.<br><br>These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br><br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br><br>Pseudonym (optional)<br><br>/T (optional)<br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory)<br><br>If serialNumber is present then it must be structured per Section 5.1.3 of ETSI EN 319 412-1: | See definitions in Section 7.1.1<br><br>Variable |

| | | |
|---|---|---|
| | 3 character identity type reference (e.g. PAS or IDC);<br>2 character ISO 3166 country code;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>identifier. | |
| SAN | /E | Optional |
| Certificate Policies | 1.3.6.1.4.1.8024.1.400 QV Qualified QSCD, or 1.3.6.1.4.1.8024.1.410 QV Qualified QSCD – on behalf of<br>0.4.0.194112.1.2 (QCP-n-qscd)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional)<br>URL: https://www.quovadisglobal.com/repository<br>User Notice: Qualified certificate | Fixed<br><br>Only Swiss Qualified |
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | digitalSignature (optional)<br>Nonrepudiation<br><br>keyEncipherment (optional) | Variable |
| Extended Key Usage | clientAuth (optional)<br>emailProtection<br>documentSigning | Variable (at least one is present) |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-4 | esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD. | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository Language = EN | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.1 (optional semantics identifier OID that is included in QuoVadis Certificates) | Fixed |

### 10.5.2. eIDAS Qualified Certificate issued to a Natural Person

| **Purpose** | | |
|---|---|---|
| The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.<br>This type of QuoVadis Qualified Certificates does not use a QSCD for the protection of the private key. The content of these Certificates meet the relevant requirements of:<br>• ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures<br>• ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons<br>• ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements | | |
| **Registration Process** | | |
| Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for the "Policy for EU qualified certificate issued to a natural person" (QCP-n). QuoVadis recommends that QCP-n certificates are used only for electronic signatures.<br>Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. Only methods approved for eIDAS Qualified Certificates may be used. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.<br>The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br>Pseudonym (optional if natural person)<br>/T (optional)<br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory)<br>If serialNumber is present then it must be structured per Section 5.1.3 of ETSI EN 319 412-1:<br>3 character identity type reference (e.g. PAS or IDC);<br>2 character ISO 3166 country code;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>identifier. | See definitions in Section 7.1.1<br>Variable |
| SAN | /E | Optional |

| | | |
|---|---|---|
| Certificate Policies | 1.3.6.1.4.1.8024.1.450 QV Qualified no QSCD, or 1.3.6.1.4.1.8024.1.460 QV Qualified no QSCD – on behalf of<br>0.4.0.194112.1.0 (QCP-n)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional)<br>URL: https://www.quovadisglobal.com/repository | Fixed |
| Key Usage (Critical) | digitalSignature (optional)<br>Nonrepudiation<br>keyEncipherment (optional) | Variable |
| Extended Key Usage | emailProtection<br>clientAuth<br>documentSigning | Variable |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository<br>Language = EN | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.1 (id-etsi-qcs-semanticsId-Natural) (optional semantics identifier OID that is included in QuoVadis Certificates) | Fixed |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |

### 10.5.3. eIDAS Qualified Certificate issued to a Legal Person on a QSCD

| **Purpose** |
|---|
| The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation. This type of QuoVadis Qualified Certificates uses a QSCD for the protection of the private key.<br>These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd). QuoVadis recommends that QCP-l-qscd certificates are used only for electronic seals.<br>The content of these Certificates meet the relevant requirements of:<br>• ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures |

- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

**Registration Process**

Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd).

Subjects may include an Organisation (legal person). Only methods approved for eIDAS Qualified Certificates may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.

Additional steps to verify PSD2 specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognised identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA (e.g,, using a national public register, EBA PSD2 Register, EBA Credit Institution Register or authenticated letter). QuoVadis also confirms the PSD2 role(s) of the Certificate Applicant (RolesOfPSP) in accordance with the rules for validation provided by the NCA, if applicable:

- i) account servicing (PSP_AS)
  OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
- ii) payment initiation (PSP_PI)
  OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
- iii) account information (PSP_AI)
  OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
- iv) issuing of card-based payment instruments (PSP_IC)
  OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }

These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

| **Attribute** | **Values** | **Comment** |
|---|---|---|
| Subject | /CN (mandatory) =/0<br>/O (optional)<br>/OU (optional)<br>/organizationalIdentifier (mandatory)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory)<br>If serialNumber is present then it must be structured per Section 5.1.3 of ETSI EN 319 412-1:<br>3 character identity type reference (e.g. PAS or IDC);<br>2 character ISO 3166 country code;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and | See definitions in Section 7.1.1<br>Variable |

| | | |
|---|---|---|
| | identifier.<br>For PSD2:<br>“PSD" as 3 character legal person identity type reference;<br>2 character ISO 3166 [7] country code representing the NCA country;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>2-8 character NCA identifier (A-Z uppercase only, no separator)<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>PSP identifier (authorisation number as specified by the NCA). | |
| SAN | /E | Optional |
| Certificate Policies | 1.3.6.1.4.1.8024.1.400 QV Qualified – QSCD or 1.3.6.1.4.1.8024.1.410 QV Qualified QSCD – on behalf of 0.4.0.194112.1.3 (QCP-l-qscd)<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>URL: https://www.quovadisglobal.com/repository | Fixed |
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | Nonrepudiation<br>digitalSignature (optional) | Variable |
| Extended Key Usage | clientAuth (optional)<br>emailProtection (optional)<br>documentSigning (optional) | Variable (at least one is present) |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)<br>id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)<br>id-etsi-qcs-4 | esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD. | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6)<br>id-etsi-qcs-6 | esi4-qcStatement-6 : Type of certificate<br>id-etsi-qcs-QcType 2 = Certificate for electronic Seals as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5)<br>id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository<br>Language = EN | Fixed |

| | | |
|---|---|---|
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is included in QuoVadis Certificates | Fixed |
| id-etsi-psd2-qcStatement (0.4.0.19495.2) | PSD2QcType ::= SEQUENCE{rolesOfPSP RolesOfPSP, nCAName NCAName,nCAId NCAId} | Only for PSD2, Variable. Refer to: ETSI TS 119 495 5.1 |

### 10.5.4. eIDAS Qualified Certificate issued to a Legal Person

| **Purpose** |
|---|
| The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.<br><br>These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person" (QCP-l). QuoVadis recommends that QCP-l certificates are used only for electronic seals. The content of these Certificates meet the relevant requirements of:<br><br>• ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures<br>• ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons<br>• ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements<br>• ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 |
| **Registration Process** |
| Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person" (QCP-l). The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:<br><br>Subjects may include an Organisation (legal person). Only methods approved for eIDAS Qualified Certificates may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature.<br><br>Additional steps to verify PSD2 specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognised identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA (e.g,, using a national public register, EBA PSD2 Register, EBA Credit Institution Register or authenticated letter). QuoVadis also confirms the PSD2 role(s) of the Certificate Applicant (RolesOfPSP) in accordance with the rules for validation provided by the NCA, if applicable:<br><br>• i) account servicing (PSP_AS)<br>OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }<br>• ii) payment initiation (PSP_PI)<br>OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }<br>• iii) account information (PSP_AI)<br>OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }<br>• iv) issuing of card-based payment instruments (PSP_IC)<br>OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 } |

| The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control. | | |
|---|---|---|
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory) =/0<br>/O (optional)<br>/OU (optional)<br>organizationalIdentifier (mandatory)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory)<br>If serialNumber is present then it must be structured per Section 5.1.3 of ETSI EN 319 412-1:<br>3 character identity type reference (e.g. PAS or IDC);<br>2 character ISO 3166 country code;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>identifier.<br>For PSD2:<br>“PSD" as 3 character legal person identity type reference;<br>2 character ISO 3166 [7] country code representing the NCA country;<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>2-8 character NCA identifier (A-Z uppercase only, no separator)<br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br>PSP identifier (authorisation number as specified by the NCA). | See definitions in Section 7.1.1<br>Variable |
| SAN | /E | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.450 QV Qualified – no QSCD or 1.3.6.1.4.1.8024.1.460 QV Qualified no QSCD – on behalf of<br>0.4.0.194112.1.1 (QCP-l)<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>URL: https://www.quovadisglobal.com/repository | Fixed |
| Key Usage (Critical) | digitalSignature (optional)<br>nonRepudiation | Variable |
| Extended Key Usage | clientAuth (optional)<br>emailProtection (optional)<br>documentSigning (optional) | Variable (at least one is present) |

| qcStatements | | |
|---|---|---|
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)<br>id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6)<br>id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate<br>id-etsi-qcs-QcType 2 = Certificate for electronic Seals as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5)<br>id-etsi-qcs-5 | URL=<br>https://www.quovadisglobal.com/repository<br>Language = EN | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is included in QuoVadis Certificates | Fixed |
| id-etsi-psd2-qcStatement<br>(0.4.0.19495.2) | PSD2QcType ::= SEQUENCE{rolesOfPSP RolesOfPSP, nCAName NCAName,nCAId NCAId} | Only for PSD2<br>Variable<br>Refer to: ETSI TS 119 495 5.1 |

### 10.5.5. QuoVadis Qualified Website Authentication Certificate (QEVCP-w)

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

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

The QuoVadis QWAC is designed to comply with:

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

| Field | Value | Comments |
|---|---|---|
| Version | V3 (2) | |
| Serial Number | Unique system generated random number assigned to each certificate, containing at least 64 bits of output. | |
| Validity Period | 397 days. | |
| **Subject Distinguished Name** | | |
| Organisation 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 Identifier | subject:organisationIdentifier (2.5.4.97) | Refer to:<br>CA/Browser Forum Ballot SC17 |
| Organisation Unit | subject:organisationUnit (2.5.6.5) | Not permitted |
| Common Name | subject:commonName (2.5.4.3)<br>cn = Common name | SubjectAlternativeName:dNSName is found below in this table.<br>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<br>Town of Incorporation | subject:jurisdictionOfIncorporationLocalityName<br>(1.3.6.1.4.1.311.60.2.1.1) | ASN.1 - X520LocalityName as specified in RFC 5280<br>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/<br>Province of Incorporation | subject:jurisdictionOfIncorporationStateOrProvinceName<br>(1.3.6.1.4.1.311.60.2.1.2) | ASN.1 - X520StateOrProvinceName as specified in RFC 5280<br>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<br>(1.3.6.1.4.1.311.60.2.1.3) | ASN.1 - X520countryName as specified in RFC 5280<br>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.<br>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;<br>Digital Signature, Key Encipherment | |
| Extended Key Usage | c=no;<br>Server Authentication (1.3.6.1.5.5.7.3.1)<br>Client Authentication (1.3.6.1.5.5.7.3.2) | |
| Certificate Policies | c=no;<br>[1] Certificate Policy: Policy Identifier=0.4.0.194112.1.4<br>[2] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.8024.0.2.100.1.2 | [1] QEVCP-W policy from ETSI EN 319 411-2<br>[2] QuoVadis EV policy OID<br>[3] QuoVadis Qualified (not on QSCD policy OID<br>[4] CAB Forum EV OID |

| | | |
|---|---|---|
| | [3] Certificate Policy:<br>Policy Identifier=<br>1.3.6.1.4.1.8024.1.450<br>[3,1] Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.quovadisglobal.com/repository<br>[4] Certificate Policy:<br>Policy Identifier=2.23.140.1.1 | |
| Certificate Transparency (optional) | (1.3.6.1.4.1.11129.2.4.4)<br>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<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/qvqwebg1.crt | |
| CRL Distribution Points | c = no; CRL HTTP URL = http://crl.quovadisglobal.com/qvqwebg1.crl | |
| cabfOrganizationIdentifier | cabfOrganizationIdentifier 2.23.140.3.1 | Optional<br>Refer to:<br>CA/Browser Forum Ballot SC17 |
| **qcStatements** | | |
| id-etsi-qcs- QcCompliance | id-etsi-qcs (1 0.4.0.1862.1.1)<br>esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Refer to:<br>ETSI EN 319 412-5 |
| id-etsi-qcs-QcType | id-etsi-qcs-6 (0.4.0.1862.1.6)<br>esi4-qcStatement-6 : Type of certificate<br>Id-etsi-qct-web (0.4.0.1862.1.6.3)<br>id-etsi-qcs-QcType 3 = Certificate for website authentication as defined in Regulation EU No 910/2014 | Refer to:<br>ETSI EN 319 412-5 |
| id-etsi-qcs-QcPDS | id-etsi-qcs-5 (0.4.0.1862.1.5)<br>URL=<br>https://www.quovadisglobal.com/re | Refer to:<br>ETSI EN 319 412-5 |

| | | |
|---|---|---|
| | pository<br>Language = EN | |
| id-qcs-pkixQCSyntax-v2 | 1.3.6.1.55.7.11.2 | |

**Verification Requirements**

The verification requirements for a QuoVadis Qualified Website Authentication (QEVCP-w) certificate are consistent with the vetting requirements for a QuoVadis EV TLS certificate, with the additional verification:

QuoVadis policy is that QuoVadis Qualified Website Authentication (QEVCP-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 using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which QuoVadis can prove the equivalence. This may include via physical presence, Remote Identity Verification (RIV4 only), or reliance on a Qualified Electronic Signature.

### 10.5.6. QuoVadis QCP-w-psd2

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

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

| **Field** | **Value** | **Comments** |
|---|---|---|
| **Subject Distinguished Name** | | |
| Organisation Identifier | subject:organizationIdentifier<br>(2.5.4.97) | PSD2 Authorisation Number<br>Refer to:<br>ETSI TS 119 495 5.1<br>CA/Browser Forum Ballot SC17 |
| **Extension** | **Value** | |
| Certificate Policies | c=no;<br>[1] Certificate Policy:<br>Policy Identifier=0.4.0.194112.1.4<br>[2] Certificate Policy:<br>Policy Identifier=<br>1.3.6.1.4.1.8024.0.2.100.1.2<br>[3] Certificate Policy:<br>Policy Identifier=<br>1.3.6.1.4.1.8024.1.450<br>[3,1] Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.quovadisglobal.com/repository<br>[4] Certificate Policy:<br>Policy Identifier=2.23.140.1.1<br>[5] Certificate Policy:<br>Policy Identifier=0.4.0.19495.3.1 | [1] QEVCP-W policy from ETSI EN 319 411-2<br>[2] QuoVadis EV policy OID<br>[3] QuoVadis Qualified (not on QSCD policy OID<br>[4] CAB Forum EV OID<br>[5] PSD2 OID QCP-w-PSD2 |

| **cabfOrganizationIdentifier** | | |
|---|---|---|
| cabfOrganizationIdentifier | cabfOrganizationIdentifier<br>2.23.140.3.1 | Refer to:<br>CA/Browser Forum Ballot SC17 |
| **qcStatements** | | |
| id-etsi-qcs- QcCompliance | id-etsi-qcs (1 0.4.0.1862.1.1)<br>esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Refer to:<br>ETSI EN 319 412-5 |
| id-etsi-qcs-QcType | id-etsi-qcs-6 (0.4.0.1862.1.6)<br>esi4-qcStatement-6 : Type of certificate<br>Id-etsi-qct-web (0.4.0.1862.1.6.3)<br>id-etsi-qcs-QcType 3 = Certificate for website authentication as defined in Regulation EU No 910/2014 | Refer to:<br>ETSI EN 319 412-5 |
| id-etsi-qcs-QcPDS | id-etsi-qcs-5 (0.4.0.1862.1.5)<br>URL= https://www.quovadisglobal.com/repository<br>Language = EN | Refer to:<br>ETSI EN 319 412-5 |
| Etsi-psd2-qcstatement | id-etsi-psd2-qcStatement<br>(0.4.0.19495.2)<br>PSD2QcType ::= SEQUENCE{<br>rolesOfPSP RolesOfPSP,<br>nCAName NCAName,<br>nCAId NCAId } | Refer to:<br>ETSI TS 119 495 5.1 |
| id-qcs-pkixQCSyntax-v2 | 1.3.6.1.55.7.11.2 | |

**Verification Requirements**

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

**Authorisation Number**

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

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

| | |
|---|---|
| | hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)) |
| | PSP identifier (Authorisation Number as specified by the NCA) |

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

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

**PSD2 Roles**

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

i) account servicing (PSP_AS)
   - OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
     Role: PSP_AS

ii) payment initiation (PSP_PI)
   - OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
     Role: PSP_PI

iii) account information (PSP_AI)
   - OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
     Role: PSP_AI

iv) issuing of card-based payment instruments (PSP_IC)
   - OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }
     Role: PSP_IC

**Revocation Requests**

Based on an authenticated request from an NCA, in accordance with ETSI TS 119 495 Section 6.2.6, QuoVadis shall revoke a PSD2 certificate within 24 hours if:

- the Authorisation of the PSP has been revoked;
- any PSP role included in the certificate has been revoked.

QuoVadis will investigate unauthenticated requests from an NCA, and shall revoke the affected certificate(s) if necessary. Unauthenticated NCA notifications need not be processed within 24 hours.

## *10.6. ZERTES QUALIFIED AND REGULATED*

### 10.6.1. Swiss Qualified Certificate

| **Purpose** | | |
|---|---|---|
| QV Swiss Qualified Certificates are Qualified personal certificates according to the Swiss Federal signature law (ZertES). They are issued out of the "QuoVadis Swiss Regulated CAs" and have the notice text "qualified certificate" in the CertificatePolicies user notice. QV Swiss Qualified Certificates are used to sign documents electronically. The Digital Signature is legally equivalent to a handwritten signature. | | |
| **Registration Process** | | |
| QV Swiss Qualified Certificates are issued in accordance with the ZertES requirements using various QuoVadis Signing Services designed for this type of Certificate. The guidelines in TAV-ZERTES apply to the specification of QV Qualified Switzerland Certificates.<br><br>Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3. Only Remote Identity Verification means approved according to ZertES may be used. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on Qualified Electronic Signature, or video verification. Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.<br><br>Private Keys for QV Swiss Qualified Certificates are generated and stored on an HSM or USB Token that meets the ZertES requirements FIPS PUB 140-2, level 3 or EAL 4 standards. HSMs for QuoVadis Signing Services are located in QuoVadis datacentres. Access by the Subscriber to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone SSCD.<br><br>QV Swiss Qualified Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br><br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br><br>Pseudonym (optional if natural person)<br><br>/T (optional)<br>/O (optional)<br>/OU (optional)<br>/organizationIdentifier (optional)<br>/serialNumber (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory)<br><br>If serialNumber is present then it must be structured per Section 5.1.3 of ETSI EN 319 412-1:<br><br>3 character identity type reference (e.g. PAS or IDC);<br><br>2 character ISO 3166 country code;<br><br>hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and<br><br>identifier. | See definitions in Section 7.1.1<br><br>Variable |

| | | |
|---|---|---|
| SAN | /E | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.400 QV Qualified – QSCD or 1.3.6.1.4.1.8024.1.410 QV Qualified QSCD – on behalf of<br>0.4.0.194112.1.2 (QCP-n-qcsd)<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional)<br>URL: https://www.quovadisglobal.com/repository<br>User Notice : qualified certificate | Fixed |
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | nonRepudiation | Fixed |
| Extended Key Usage | emailProtection<br>documentSigning | Fixed |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)<br>id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed: issued before January 13, 2021 |
| id-etsi-qcs-QcCClegislation (0.4.0.1862.1.7)<br>id-etsi-qcs-7 | esi4-qcStatement-7: Claim that the certificate is a Swiss Qualified Certificate (CH) | Fixed: issued after January 13, 2021 |
| id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)<br>id-etsi-qcs-4 | esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD. | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5)<br>id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository<br>Language = en | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.2 (optional semantics identifier OID that is included in QuoVadis Certificates) | Fixed |

### 10.6.2. Swiss Regulated Certificate issued to a Natural Person

| **Purpose** | | |
|---|---|---|
| Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ Certificate Class. They are issued out of Swiss Regulated CAs and have the notice text "regulated certificate" in the CertificatePolicies user notice. Swiss Qualified Certificates are described in a separate Section of this CP/CPS. | | |
| **Registration Process** | | |
| Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates.<br><br>For the issuance and life cycle management of Swiss Regulated Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES Qualified Certificate.<br><br>Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries). Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.<br><br>These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or is used) under the Subject's sole control.<br><br>Swiss Regulated Certificates have a maximum validity of three years. | | |
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN or Pseudonym)<br><br>/GN (mandatory if CN without Pseudonym)<br>/SN (mandatory if CN without Pseudonym)<br><br>Pseudonym (optional for natural person)<br><br>/T (optional)<br>/O (optional)<br>/OU (optional)<br>/organizationIdentifier (optional)<br>/E (optional)<br>/L (optional) /ST (optional) /C (mandatory) | See definitions in Section 7.1.1<br><br>Variable |
| SAN | /E<br>1.3.6.1.4.1.311.20.2.3 UPN | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.300 QV Advanced+ Certificate<br>0.4.0.2042.1.2 ETSI NCP+ OID<br>2.23.140.1.5.3.1 S/MIME Sponsor-Legacy (optional)<br>2.23.140.1.5.4.1 S/MIME Individual-Legacy (optional)<br><br>URL:<br>https://www.quovadisglobal.com/repository<br><br>User Notice: Regulated certificate | Fixed |

| | | |
|---|---|---|
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | digtalSignature | Fixed |
| Extended Key Usage | clientAuth<br>emailProtection<br>smartcardlogon | Fixed |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-4 | esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD. | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository Language = en | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.1 (optional semantics identifier OID that is included in QuoVadis Certificates) | Fixed |

### 10.6.3. Swiss Regulated Certificate issued to a Legal Person (Company Seal)

| **Purpose** |
|---|
| Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QV Advanced+ Certificate Class. They are issued out of Swiss Regulated CAs and have the notice text "regulated certificate" in the CertificatePolicies user notice. Swiss Qualified Certificates are described in a separate Section of this CP/CPS. |
| **Registration Process** |
| Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates.<br>For the issuance and life cycle management of Swiss Regulated Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant Qualified Certificate.<br>Subjects may include an Organisation (legal person). Only methods approved for ZertES may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries).<br>Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.<br>These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or is used) under the Subject's sole control. |

| Swiss Regulated Certificates have a maximum validity of three years. | | |
|---|---|---|
| **Attribute** | **Values** | **Comment** |
| Subject | /CN (mandatory) = /O<br>/O (mandatory)<br>/OU (optional)<br>/organizationIdentifier (mandatory)<br>/E (optional)<br>/L /ST (optional)<br>/C (mandatory) | See definitions in Section 7.1.1<br>Variable |
| SAN | /E | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.300 QV Advanced+ Certificate<br>0.4.0.2042.1.2 ETSI NCP+ OID<br>2.23.140.1.5.2.1 S/MIME Org-Legacy (optional)<br>URL:<br>https://www.quovadisglobal.com/repository<br>User Notice: Regulated certificate | Fixed |
| Adobe Acrobat Trust List | 1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA)<br>1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation) | Optional |
| Key Usage (Critical) | digitalSignature | Fixed |
| Extended Key Usage | emailProtection<br>documentSigning | Fixed |
| **qcStatements** | | |
| id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1 | esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-4 | esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD. | Fixed |
| id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6 | esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014 | Fixed |
| id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5 | URL= https://www.quovadisglobal.com/repository Language = en | Fixed |
| id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) | 0.4.0.194121.1.1 (optional semantics identifier OID that is included in QuoVadis Certificates) | Fixed |

## *10.7. QV CLOSED COMMUNITY*

Closed Community Issuing CAs can, under contract, create Certificate Profiles for the issuance of Certificates to members of that community.

Certificates issued by Closed Community Issuing CAs are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone CP/CPS to its community issue various Certificates in accordance with the CP/CPS.

QuoVadis must approve all closed community Certificate policies to ensure that they do not conflict with the terms of the relevant CP/CPS and also industry standards. Under no circumstances can Closed Community Issuing CAs issue Qualified Certificates under the Swiss Digital Signature law.

### 10.7.1. Grid Certificates

This Section provides an overview of the requirements and Certificate contents for Grid Certificates issued in accordance with the requirements of the International Grid Trust Federation (IGTF) or one of its member bodies.

All Grid End User Certificates and Grid Server Certificates issued must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

All Grid Certificates will be issued to Applicants based on cryptographic data generated by the Applicant, or based on cryptographic data that can be held only by the Applicant on a secure hardware token. Any single Subject Distinguished Name must be linked to one and only one entity and must not be linked to any other entity over the life of the CA. Pseudonyms will not be allowed for Grid Certificates. Private Key archival or escrow is forbidden for all Grid Certificates. Revocation requests must be properly authenticated before they are accepted. Revocation requests can be made by end entities, RAs and QuoVadis. Others can also request revocation if they can sufficiently prove compromise of the associated Private Key. Subscribers must request revocation as soon as possible. This should be within one working day after detection of loss or compromise of the Private Key pertaining to the Certificate, or if the data in the Certificate is no longer valid. Proxy Certificates will be supported in relation to Grid Certificate. A Grid Certificate must be revoked if a related Proxy Certificate is compromised in any way. The maximum Certificate Revocation List lifetime for Grid Certificates is 30 days.

Grid Certificate Re-Keying can only take place if the Subscriber is already in possession of a valid Grid Certificate and uses this Certificate to submit the Re-Key request. Certificates can only be Re-Keyed for up to a maximum of 3 years, after which period the Subscriber is required to apply for a new Certificate. If the Subscriber has lost their Private Key, or if their existing Certificate has expired, they will need to apply for new Certificate.

#### *10.7.1.1. Grid End User Certificate*

| **Purpose** |
|---|
| Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid End User Certificate is to help the Subscriber to access the Grid services that require Certificate-based authentication. |
| **Registration Process** |
| The identity vetting of all Applicants must be performed by an approved RA. Face to face registration is required at the RA or alternatively the Applicants can have their identity vetted at a post office providing an approved identity vetting service. The Applicant must present a valid photo ID and/or valid official documents in accordance with formally documented RA procedures. The RA is responsible for recording, at the time of validation, sufficient information regarding the Applicant to identify the Applicant. The RA is responsible for maintaining documented evidence on retaining the same identity over time. The Certificate request submitted for certification must be bound to the act of identity vetting. |
| **Digital Certificate Delivery** |

| All successful Grid End User Certificate Requests will be processed by the QuoVadis Grid Issuing CA. QuoVadis will not generate the Private Keys for Grid End User Certificates. If software tokens are used, the Private Key must be protected with a strong pass phrase that follows current best practices for choosing high-quality passwords. | | |
|---|---|---|
| **Attribute** | **Values** | **Comment** |
| Issuer | /CN = Variable<br>/O = QuoVadis Limited /C = BM | Fixed |
| Validity | Maximum Certificate lifetime of 1 year | Fixed |
| Subject | /CN (mandatory)<br>= Natural Person (/GN+/SN)<br>/O (mandatory) /OU (optional)<br>/L (optional)<br>/ST (optional)<br>/C (mandatory) | See definitions in Section 7.1.1<br>Variable |
| Domain Components (DC) | DC=com, DC=quovadisglobal, DC=grid, DC=<organisation identifier>, DC=users | Holder Variable |
| SAN | /E | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.0.1.10.0.0 QV Grid<br>1.2.840.113612.5.2.2.1 IGTF Classic Authentication Profile | Fixed |
| Key Usage (Critical) | digitalSignature<br>keyEncipherment<br>dataEncipherment | Fixed |
| Extended Key Usage | clientAuth<br>emailProtection | Fixed |

#### *10.7.1.2. Grid Server Certificate*

| **Purpose** | | |
|---|---|---|
| Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid Server Certificate is to help secure communications with Grid servers. | | |
| **Registration Process** | | |
| The identity vetting of all Applicants must be performed by an approved RA. For Grid Server Certificates, the RA must validate the identity and eligibility of the person in charge of the specific entities using a secure method. The RA is responsible for recording, at the time of validation, sufficient information regarding the Applicant to identify the Applicant.<br>As part of the registration process the RA must ensure that the Applicant is appropriately authorised by the owner of the associated Fully Qualified Domain Name (FQDN) or the responsible administrator of the machine to use the FQDN identifiers asserted in the Certificate. The RA is responsible for maintaining documented evidence on retaining the same identity over time.<br>The RA must validate the association of the Certificate Signing Request. The Certificate Request submitted for certification must be bound to the act of identity vetting. | | |
| **Digital Certificate Delivery** | | |
| Private Keys pertaining to Grid Server Certificates may be stored without a passphrase, but must be adequately protected by system methods if stored without passphrase. | | |
| **Attribute** | **Values** | **Comment** |

| | | |
|---|---|---|
| Issuer | /CN = Variable<br>/O = QuoVadis Limited<br>/C = BM | Fixed |
| Validity | Maximum Certificate lifetime of 1 year | Fixed |
| Subject | /CN<br>/O (mandatory)<br>/L (optional)<br>/ST (optional)<br>/C (mandatory) | See definitions in Section 7.1.1<br>Variable |
| Domain Components (DC) | DC=com, DC=quovadisglobal, DC=grid, DC=<organisation identifier>, DC=hosts | Holder Variable |
| SAN | SAN dNSName with the Fully Qualified Domain Name or an iPAddress | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.0.1.10.0.0 QV Grid<br>1.2.840.113612.5.2.2.1 IGTF Classic Authentication Profile<br>2.23.140.1.2.2 CABF OV | Fixed |
| Key Usage (Critical) | digitalSignature<br>keyEncipherment | Fixed |
| Extended Key Usage | clientAuth<br>serverAuth | Fixed |

## *10.8. QUOVADIS DEVICE*

| **Purpose** | | |
|---|---|---|
| QuoVadis Device Certificates are intended for a variety of uses including for Time-stamp Authority (TSA) applications. QuoVadis Device Certificates that have the serverAuth EKU comply with the TLS BR. | | |
| **Registration Process** | | |
| QuoVadis acts as RA for Device Certificates it issues. Before issuing a Device Certificate, QuoVadis performs procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and/or Organisation name to be included in the Certificate, and has accepted a Subscriber Agreement for the requested Certificate.<br><br>Documentation requirements for organisation Applicants may include, Certificate of Incorporation, Memorandum of Association, Articles of Incorporation or equivalent documents. Documentation requirements for individual Applicants may include trustworthy, valid photo ID issued by a Government Agency (such as a passport). QuoVadis may accept at its discretion other official documentation supporting an application. | | |
| Key Usage (Critical) | Depends on the type of Certificate. | Variable |
| Extended Key Usage | Depends on the type of Certificate. | Variable |
| Subject Alternative Name | If the serverAuth EKU is present then this field must contain either a dNSName containing the Fully- Qualified Domain Name or an iPAddress containing the IP address of a server. | Variable |
| Certificate Policies | 1.3.6.1.4.1.8024.1.600 QV Device Certificate<br><br>If the serverAuth EKU is present:<br>= 2.23.140.1.2.2<br><br>If the serverAuth EKU is present, either: = 1.3.6.1.4.1.8024.0.1.100.1.1 (if chains to QV Root 1), OR = 1.3.6.1.4.1.8024.0.3.100.1.1 (if chains to QV Root 3)<br><br>If the codeSigning EKU is present:<br>= 2.23.140.1.2.3<br><br>If the timeStamping EKU is present, operated by QuoVadis:<br>1.3.6.1.4.1.8024.0.2000.6 | Variable |
| Certificate Transparency | (1.3.6.1.4.1.11129.2.4.4)<br><br>If the serverAuth EKU is present, this field MAY include two or more Certificate Transparency proofs from approved CT Logs. | Optional |

## *10.9. TLS CERTIFICATES*

### 10.9.1. OV - Business TLS

| **Field** | **Value** |
|---|---|
| Validity Period | 397 days |
| **Subject Distinguished Name** | |
| Organisation Name | subject:organisationName (2.5.4.10 ) |
| Organisation Unit | subject:organisationUnit (2.5.6.5)<br>Discontinued effective August 31, 2020. |
| Common Name | subject:commonName (2.5.4.3)<br>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;<br>Digital Signature, Key Encipherment |
| Extended Key Usage | c=no;<br>serverAuth (1.3.6.1.5.5.7.3.1)<br>clientAuth (1.3.6.1.5.5.7.3.2) |
| Certificate Policies | c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.1.100.1.1 or 1.3.6.1.4.1.8024.0.3.100.1.1 or 1.3.6.1.4.1.8024.0.2.100.1.1} Certificate Policies; {2.23.140.1.2.2}<br>[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)<br>This field MAY include two or more Certificate Transparency proofs from approved CT Logs. |

**Purposes of Business TLS**

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

**Verification Requirements**

Identity: QuoVadis verifies the identity and address of the organisation 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:

i) A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

ii) A third party database that is periodically updated and considered a Reliable Data Source;

iii) A site visit by the CA or a third party who is acting as an agent for the CA; or

iv) 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:

i) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

ii) A Reliable Data Source;

iii) Communication with a government agency responsible for the management of such DBAs or tradenames;

iv) An Attestation Letter accompanied by documentary support; or

v) 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:

i) the IP Address range assignment by country for either (i) the web site's IP

ii) address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;

iii) the ccTLD of the requested Domain Name;

iv) information provided by the Domain Name Registrar; or

v) 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 TLS Certificate, along with a PKCS#10 CSR and billing details.

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

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

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

Step 6: QuoVadis creates the Business TLS Certificate.

Step 7: The Business TLS 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.

### 10.9.2. EV - Extended Validation TLS

| Field | Value | Comments |
|---|---|---|
| Validity Period | 397 days | |
| **Subject Distinguished Name** | | |
| 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. | subject:organisation Name (2.5.4.10 ) |
| organisationUnit (2.5.6.5) | Not permitted in QuoVadis EV TLS. | subject:organisation Unit (2.5.6.5) |
| commonName (2.5.4.3)<br>cn = Common name | SubjectAlternativeName:dNSName is found below in this table.<br>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. | subject:commonNam e (2.5.4.3)<br>cn = Common name |
| Organisation Identifier (2.5.4.97)<br>(optional) | subject:organizationIdentifier (2.5.4.97) | Refer to: CA/Browser Forum Ballot SC17 |
| jurisdictionOfIncorporatio nLocalityName (1.3.6.1.4.1.311.60.2.1.1) | ASN.1 - X520LocalityName as specified in RFC 5280<br>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. | subject:jurisdictionO fIncorporationLocalit yName (1.3.6.1.4.1.311.60.2. 1.1) |

| | | |
|---|---|---|
| jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) | ASN.1 - X520StateOrProvinceName as specified in RFC 5280<br>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. | subject:jurisdictionOfIncorporationStateOrProvin ceName (1.3.6.1.4.1.311.60.2.1.2) |
| jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) | ASN.1 - X520countryName as specified in RFC 5280<br>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.<br>Country information MUST be specified using the applicable ISO country code. | subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) |
| 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". | Subject:serialNumber (2.5.4.5) |
| 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. | Subject:businessCategory (2.5.4.15) |
| 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 or 3072-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;<br>Server Authentication (1.3.6.1.5.5.7.3.1)<br>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 }<br>Certificate Policies; { 2.23.140.1.1}<br>[1,1] Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.quovadisglobal.com/repository<br>[1,2] Policy Qualifier Info:<br>Policy Qualifier Id=User Notice<br>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)<br>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<br>=http://crl.quovadisglobal.com/QVSSLICA.crl or http://crl.quovadisglobal.com/qvsslg2.crl or http://crl.quovadisglobal.com/qvsslg3.crl | |
| cabfOrganizationIdentifier | cabfOrganizationIdentifier<br>2.23.140.3.1 | Optional<br>Refer to:<br>CA/Browser Forum Ballot SC17 |

**Purpose of EV TLS**

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

**Eligible Applicants**

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

i) Private Organisation Subjects

- The Private Organisation 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 Organisation 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 Organisation 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 Organisation MUST have a verifiable physical existence and business presence.
- The Private Organisation'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 or the United States; and
- The Private Organisation MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda or the United States.

ii) Government Entity Subjects

- The legal existence of the Government Entity MUST be established by the political subdivision in which it operates;
- The Government Entity MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a Certificate by the laws of Bermuda or the United States; 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 or the United States.

iii) Business Entity Subjects

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

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

- Where the Business Entity represents itself under an assumed name, QuoVadis MUST verify the Business Entity's use of the assumed name;
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where QuoVadis is prohibited from doing business or issuing a Certificate under the laws of Bermuda or the United States; 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 or the United States.

iv) 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 Organisation 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 Organisation Entity MUST NOT be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of Bermuda or the United States; and
- The International Organisation Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda or the United States.
- Subsidiary organisations or agencies of qualified International Organisations 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 Subscribers, Certificate Subjects, Application Software Vendors with whom QuoVadis has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors, and all Relying Parties that actually rely on such EV Certificate during the period when it is valid, that it followed the requirements of the EV Guidelines and this CP/CPS in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (EV Certificate Warranties).

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

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

- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with QuoVadis that satisfies the requirements of the EV Guidelines or the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: QuoVadis will follow the requirements of the EV Guidelines and maintains a 24/7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or Revoked; and
- 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 authorisation 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 Subscriber 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 Subscriber, 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 authorise one individual to occupy two or more of these roles. The Applicant may authorise 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 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 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 authorised agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
- Confirming Person: Must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) able to sign the QV Authority Letter on behalf of the Applicant.

**Subscriber Agreement**

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

- 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 Subscriber 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 Subscriber 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 Subscriber'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 Subscriber 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 Subscriber 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.

## *10.10. CODE SIGNING*

| **Field** | **Value** | **Comments** |
|---|---|---|
| Validity Period | 1, 2, or 3 years expressed in UTC format | |
| **Subject Distinguished Name** | | |
| Organisation Name | subject:organisationName (2.5.4.10 ) | Required field. The Subject's verified legal name. |
| Organisation Unit | subject:organisationUnit (2.5.6.5) | Optional field. Must not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless QuoVadis has verified this information |
| Common Name | subject:commonName (2.5.4.3) | Required field. The Subject's verified legal name. |
| State or province (if any) | subject:stateOrProvinceName (2.5.4.8) | Required if the subject:localityName field is absent. Optional if the subject:localityName fields is present. |
| Locality | subject:locality (2.5.4.6) | Required if the subject:stateOrProvinceName |

| | | |
|---|---|---|
| | | field is absent. Optional if the subject:stateOrProvinceName field is present. |
| Country | subject:countryName (2.5.4.6) | Required field. |
| 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;<br>digitalSignature (80) | |
| Extended Key Usage | c=no;<br>1.3.6.1.5.5.7.3.3 (codeSigning) | |
| **Field** | **Value** | **Comments** |
| Certificate Policies | c=no;<br>Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 }<br>Certificate Policies; { 2.23.140.1.4.1 }<br>[1,1] Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier: http://www.quovadisglobal.com/repository | 1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID.<br>2.23.140.1.2.3 is the Code Signing Baseline 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<br>- id-ad-caIssuers (CA Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/<CA Name>.crt | |
| CRL Distribution Points | c = no; CRL HTTP URL =http://crl.quovadisglobal.com/<CA Name>.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**

Eligible Applicants include Individual Applicants and Organisational 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 organisations, trade associations, and other entities.

**Private Key Protection**

Subscriber 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 Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

**Verification Requirements**

Before issuing a Code Signing Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to sign code in the name to be included in the Certificate.

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

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

ii) Verifies the Subject's legal identity, including any Doing Business As (DBA) as described in Section 3.2.2.2 of the TLS BR,

iii) Verifies the Subject's address, and

iv) Verifies the Certificate Requester's authority to request a Certificate and the authenticity of the Certificate Request using a verified method of communication.

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

i) Verifies the Subject's identity using a government photo ID,

ii) Verifies the Subject's address using reliable data sources,

iii) Obtains a biometric associated with the Subject, such as a fingerprint or notarised handwritten Declaration of Identity,

iv) Verifies the Certificate Requester's authority to request a Certificate and the authenticity of the Certificate Request using a verified method of communication.

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

i) the identity of the person performing the verification,

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

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

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

v) the date and time of the verification, and

vi) a declaration of identity by the Applicant that is signed in handwriting in the presence of the person performing the verification.

**Application Process**

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

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

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

Step 3: The Applicant accepts the Subscriber Agreement and approves Certificate issuance.

Step 4: All signatures are verified through follow-up procedures or telephone calls.

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

Step 6: QuoVadis creates the Code Signing Certificate.

Step 7: The Certificate is delivered to the Applicant.