digicert + QuoVadis

QuoVadis Root Certification Authority Certificate Policy/ Certification Practice Statement

OIDs:	1.3.6.1.4.1.8024.0.1 1.3.6.1.4.1.8024.0.3
Effective Date:	June 6, 2019
Version:	4.26

Important Note About this Document

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

This document covers aspects of the QuoVadis PKI that relate to all CAs established by QuoVadis under the QuoVadis Root Certification Authority and the QuoVadis Root Certification Authority 3 (QuoVadis Root CA 3). There are a number of instances where the legal and regulatory framework regarding the issuance of Qualified Certificates under the Swiss, Dutch or European 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. Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS Regulation”) came into force on 1 July 2016. For existing Certification Providers issuing Qualified Certificates the eIDAS Regulation provides for a transition period up until 1 July 2017. Following QuoVadis’ updated accreditation as a Qualified TSP it is anticipated that the specific regulations for the Netherlands and Belgium will be made consistent with eIDAS.

This flag denotes a provision relating to Qualified Certificates issued in accordance with Swiss regulations.

This flag denotes a 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:

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

Website: http://www.quovadisglobal.com

e-mail: compliance@quovadisglobal.com

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

Version Control

Author	Date	Version	Comment
QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	WebTrust Revisions
QuoVadis PMA	01 April 2004	2.07	WebTrust Revisions
QuoVadis PMA	11 November 2005	2.08	WebTrust Revisions
QuoVadis PMA	17 April 2006	4.00	Cumulative ZertES Revisions
QuoVadis PMA	14 September 2006	4.1	EIDI-V Certificate Requirements
QuoVadis PMA	26 February 2007	4.2	QuoVadis Root CA 3 Added
QuoVadis PMA	03 April 2007	4.3	Clarifications to Appendix A
QuoVadis PMA	29 October 2007	4.4	General Edits and RFC3647 Conformity, Cumulative ZertES and EIDI-V Revisions
QuoVadis PMA	27 May 2008	4.5	Addition for QV EU Qualified ICA and ETSI conformance
QuoVadis PMA	20 April 2009	4.6	Additions for Grid Certificates
QuoVadis PMA	22 April 2010	4.7	Updates to QuoVadis Certificate Classes and Appendix A. Includes SuisseID certificates.
QuoVadis PMA	16 November 2010	4.8	Certificate loss limits for SuisseID IAC Certificates
QuoVadis PMA	1 March 2012	4.9	Addition of restrictions for use of Issuing CAs for Man in the Middle (MITM) purposes

QuoVadis PMA	12 July 2012	4.10	Amendments reflecting requirements for Approved Client Issuing CAs and the CA/B Forum Baseline Requirements
QuoVadis PMA	31 January 2013	4.11	Updates for SHA256 Roots
QuoVadis PMA	22 May 2013	4.12	Addition of 'QCP Public' Policy
QuoVadis PMA	12 October 2013	4.13	Updates to Device Certificate section and Grid Server Profile in Appendix A
QuoVadis PMA	11 March 2014	4.14	Updates to Device Certificate section and physical controls section
QuoVadis PMA	27 May 2014	4.15	Updates to links to QuoVadis Website and archive periods
QuoVadis PMA	4 August 2014	4.16	Updates for Belgium accreditation. Minor clarifications to Grid Certificate Profile tables
QuoVadis PMA	15 April 2015	4.17	Updates to Certification Authority Authorisation (CAA) policy
QuoVadis PMA	2 December 2015	4.18	Updates relating to Swiss Qualified Certificates
QuoVadis PMA	2 August 2016	4.19	Updates for Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation")
QuoVadis PMA	8 May 2017	4.20	Updates for the eIDAS Regulation; includes Legal Person Certificates Updates for Code Signing Minimum Requirements
QuoVadis PMA	6 September 2017	4.21	Updates for Certificate Authority Authorisation (CAA). Updates for submission of complaints.
QuoVadis PMA	31 January 2018	4.22	Updates for the Baseline Requirements and Mozilla Root Store Policy
QuoVadis PMA	25 July 2018	4.23	Updates for Certificate Renewal. Additions in Appendix A relating to Qualified Certificate QSCD, where the device is managed by QuoVadis on behalf of the subject. (OID = 1.3.6.1.4.1.8024.1.410).
QuoVadis PMA	30 July 2018	4.24	Updates for domain vetting (ballot 218)

QuoVadis PMA	7 December 2018	4.25	Updates to include changes for EU Qualified certs and itsme Sign Issuing CA G1. More explicit reference to the BR Domain Vetting methods.
QuoVadis PMA	6 June 2019	4.26	Updates for where QSCD managed on behalf of Certificate Holder by QuoVadis. Updates to revocation requests. Updates for Baseline Requirements domain and IP address validation methods. Change to CRL update frequency.

Table of Contents

1 Introduction 14
1.1 Overview 14
1.2 Document Name, Identification and Applicability 17
1.3 Public Key Infrastructure Participants 17
1.3.1 Certification Authorities 19
1.3.2 Registration Authorities and Their Obligations 22
1.3.3 Certificate Holders 23
1.3.4 Relying Parties 25
1.3.5 Other Participants 27
1.4 Certificate Usage 27
1.4.1 Appropriate Certificate Usage 27
1.4.2 Prohibited Certificate Usage 28
1.5 Policy Administration 28
1.5.1 Organisation Administering the CP/CPS 28
1.5.2 Contact Person 28
1.5.3 Person Determining the CP/CPS Suitability 28
1.5.4 CP/CPS Approval Procedures 28
1.6 Definitions and Acronyms 29
2 Publication and Repository Responsibilities 29
2.1 Repositories 29
2.2 Publication of Certificate Information 29
2.3 Time or Frequency of Publication 30
2.4 Access Controls on Repositories 30
3 Identification and Authentication 30
3.1 Naming 31
3.1.1 Types Of Names 31
3.1.2 Need For Names To Be Meaningful 32
3.1.3 Pseudonymous Certificate Holders 32
3.1.4 Rules For Interpreting Various Name Forms 32
3.1.5 Uniqueness Of Names 32
3.1.6 Recognition, Authentication, And Role Of Trademarks 33
3.2 Initial Identity Validation 33
3.2.1 Method To Prove Possession Of Private Key 33
3.2.2 Authentication Of Organisation Identity 33
3.2.3 Authentication Of Individual Identity 36
3.2.4 Non-Verified Certificate Holder Information 36
3.2.5 Validation Of Authority 37
3.2.6 Criteria For Interoperation 37

3.3 Identification And Authentication For Renewal Requests 37
3.3.1 Identification and Authentication For Routine Re-Key 37
3.3.2 Identification and Authentication For Re-Key After Revocation 37
3.4 Identification and Authentication For Revocation Requests 38
3.4.1 Issuing Certification Authority 38
3.4.2 Registration Authority 38
3.4.3 Certificate Holder 38
4 Certificate Life-Cycle Operation Requirements 39
4.1 Certificate Application 39
4.1.1 Who Can Submit A Certificate Application 39
4.1.2 Enrolment Process And Responsibilities 39
4.2 Certificate Application Processing 40
4.2.1 Performing Identification And Authentication Functions 40
4.2.2 Approval Or Rejection Of Certificate Applications 40
4.2.3 Time To Process Certificate Applications 40
4.2.4 Certificate Authority Authorisation (CAA) 40
4.3 Certificate Issuance 41
4.3.1 Certification Authority Actions During Certificate Issuance 41
4.3.2 Notification To Applicant Certificate Holder By The Certification Authority Of Issuance Of Certificate 42
4.4 Certificate Acceptance 42
4.4.1 Notice Of Acceptance 43
4.4.2 Conduct Constituting Certificate Acceptance 43
4.4.3 Publication Of The Certificate By The Certification Authority 44
4.4.4 Notification Of Certificate Issuance By The Certification Authority To Other Entities 44
4.5 Key Pair And Certificate Usage 44
4.5.1 Certificate Holder Private Key And Certificate Usage 44
4.5.2 Relying Party Public Key And Certificate Usage 44
4.6 Certificate Renewal 45
4.7 Certificate Re-Key 45
4.7.1 Circumstance For Certificate Re-Key 45
4.7.2 Who May Request Re-Key 45
4.7.3 Processing Certificate Re-Key Request 45
4.7.4 Notification Of New Certificate Issuance To Certificate Holder 46
4.7.5 Conduct Constituting Acceptance Of A Re-Key Certificate 46
4.7.6 Notification Of Certificate Re-Key By The Certification Authority To Other Entities 46
4.8 Certificate Modification 46
4.9 Certificate Revocation And Suspension 46
4.9.1 Circumstances For Revocation 46
4.9.2 Who Can Request Revocation 49
4.9.3 Procedure For Revocation Request 50

4.9.4 Revocation Request Grace Period 50
4.9.5 Time Within Which The Certification Authority Must Process The Revocation Request 50
4.9.6 Revocation Checking Requirement For Relying Parties 51
4.9.7 Certificate Revocation List Issuance Frequency 51
4.9.8 Maximum Latency For Certificate Revocation List 51
4.9.9 On-Line Revocation/Status Checking Availability 51
4.9.10 On-Line Revocation Checking Requirement 51
4.9.11 Other Forms Of Revocation Advertisements Available 51
4.9.12 Special Requirements in Relation to Key Compromise 52
4.9.13 Circumstances For Suspension 52
4.9.14 Who Can Request Suspension 52
4.9.15 Procedure For Suspension Request 52
4.9.16 Limits On Suspension Period 52
4.10 Certificate Status Services 52
4.10.1 Operational Characteristics 52
4.10.2 Service Availability 52
4.10.3 Optional Features 52
4.11 End Of Subscription 52
4.12 Key Archival And Recovery 53
4.12.1 Key Archival And Recovery Policy And Practices 53
4.12.2 Session Key Encapsulation And Recovery Policy And Practices 54
5 Facility, Management, And Operational Controls 55
5.1 Physical Controls 55
5.1.1 Site Location and construction 55
5.1.2 Physical Access 55
5.1.3 Power and Air-Conditioning 56
5.1.4 Water Exposures 56
5.1.5 Fire Prevention and Protection 56
5.1.6 Media Storage 56
5.1.7 Waste Disposal 56
5.1.8 Off-Site Backup 56
5.2 Procedural Controls 57
5.2.1 Trusted Roles 57
5.2.2 Number of Persons Required Per Task 57
5.2.3 Identification and Authentication For Each Role 58
5.2.4 Roles Requiring Separation of Duties 58
5.3 Personnel Controls 58
5.3.1 Qualifications, Experience, and Clearance Requirements 59
5.3.2 Background Check Procedures 59
5.3.3 Training Requirements 59
5.3.4 Retraining Frequency And Requirements 59
5.3.5 Job Rotation Frequency And Sequence 59

5.3.6 Sanctions for Unauthorised Actions 60
5.3.7 Independent Contractor Requirements 60
5.3.8 Documentation Supplied To Personnel 60
5.4 Audit Logging Procedures 60
5.4.1 Types Of Events Recorded 60
5.4.2 Frequency Of Processing Log 61
5.4.3 Retention Period For Audit Log 61
5.4.4 Protection Of Audit Log 61
5.4.5 Audit Log Backup Procedures 61
5.4.6 Audit Collection System 61
5.4.7 Notification To Event-Causing Subject 62
5.4.8 Vulnerability Assessment 62
5.5 Records Archival 62
5.5.1 Types Of Records Archived 62
5.5.2 Retention Period For Archive 62
5.5.3 Protection Of Archive 62
5.5.4 Archive Backup Procedures 63
5.5.5 Requirements For Time-Stamping Of Records 63
5.5.6 Archive Collection System 63
5.5.7 Procedures To Obtain And Verify Archive Information 63
5.6 Key Changeover 63
5.7 Compromise And Disaster Recovery 64
5.7.1 QuoVadis Business Continuity Plan 64
5.8 Certification Authority And/Or Registration Authority Termination 64
5.8.1 User Keys And Certificates 65
5.8.2 Successor Issuing Certification Authority 65
6 Technical Security Controls 66
6.1 Key Pair Generation And Installation 66
6.1.1 Key Pair Generation 66
6.1.2 Private Key Delivery To Certificate Holder 67
6.1.3 Public Key Delivery To Certificate Issuer 67
6.1.4 Certification Authority Public Key To Relying Parties 67
6.1.5 Key Sizes 67
6.1.6 Public Key Parameters Generation And Quality Checking 68
6.1.7 Key Usage Purposes (As Per X.509 V3 Key Usage Field) 68
6.2 Private Key Protection And Cryptographic Module Engineering Controls 68
6.2.1 Cryptographic Module Standards And Controls 69
6.2.2 Private Key (N Out Of M) Multi-Person Control 69
6.2.3 Private Key Escrow 69
6.2.4 Private Key Backup 70
6.2.5 Private Key Archive 70
6.2.6 Private Key Transfer Into Or From A Cryptographic Module 70
6.2.7 Private Key Storage On Cryptographic Module 70

6.2.8 Method Of Activating Private Key 71
6.2.9 Method Of Deactivating Private Key 71
6.2.10 Method Of Destroying Private Key 71
6.2.11 Cryptographic Module Rating 71
6.3 Other Aspects Of Key Pair Management 72
6.3.1 Public Key Archival 72
6.3.2 Certificate Operational Periods And Key Pair Usage Periods 72
6.4 Activation Data 72
6.4.1 Activation Data Generation And Installation 72
6.4.2 Activation Data Protection 73
6.4.3 Other Aspects Of Activation Data 73
6.5 Computer Security Controls 73
6.5.1 Specific Computer Security Technical Requirements 73
6.5.2 Computer Security Rating 73
6.6 Life Cycle Technical Controls 74
6.6.1 System Development Controls 74
6.6.2 Security Management Controls 74
6.6.3 Life Cycle Security Controls 74
6.7 Network Security Controls 75
6.8 Time-Stamping 75
7 Certificate, CRL, And OCSP Profiles For Certificates Which Do Not Include Server Authentication Key Use 76
7.1 Certificate Profile 76
7.1.1 Basic Certificate Contents 76
7.1.2 Certificate Extensions 77
7.1.3 Algorithm Object Identifiers 79
7.1.4 Name Forms 79
7.1.5 Name Constraints 80
7.1.6 CP/CPS Object Identifier 80
7.1.7 Usage Of Policy Constraints Extension 80
7.1.8 Policy Qualifiers Syntax And Semantics 80
7.1.9 Processing Semantics For The Critical Certificate Policies Extension 80
7.2 Certificate Revocation List Profile 80
7.2.1 Version Number 81
7.2.2 Certificate Revocation List And Certificate Revocation List Entry Extensions 81
7.3 Online Certificate Status Protocol Profile 81
7.3.1 Online Certificate Status Protocol Version Numbers 81
7.3.2 Online Certificate Status Protocol Extensions 81
7.4 Lightweight Directory Access Protocol Profile 81
7.4.1 Lightweight Directory Access Protocol Version Numbers 81
7.4.2 Lightweight Directory Access Protocol Extensions 81
7.5 Digital Certificate Fields and Root CA Certificate Hashes 82

7.5.1 Digital Certificate Fields 82
7.5.2 QuoVadis Root Certificate Hashes 83
8 Compliance Audit and Other Assessments 85
8.1 Frequency, Circumstance And Standards Of Assessment 85
8.1.1 QuoVadis Certification Authority 85
8.1.2 Issuing Certification Authorities 87
8.1.3 Registration Authorities 87
8.2 Identity And Qualifications Of Assessor 87
8.3 Assessor's Relationship To Assessed Entity 87
8.4 Topics Covered By Assessment 87
8.5 Actions Taken As A Result Of Deficiency 88
8.5.1 Issuing Certification Authorities 88
8.5.2 Registration Authorities 88
8.6 Publication Of Audit Results 89
8.7 Self Audits 89
9 OTHER BUSINESS AND LEGAL MATTERS 90
9.1 Fees 90
9.1.1 Certificate Issuance Or Renewal Fees 90
9.1.2 Certificate Access Fees 90
9.1.3 Revocation Or Status Information Access Fees 90
9.1.4 Fees For Other Services 90
9.1.5 Refund Policy 90
9.2 Financial Responsibilities 91
9.2.1 Insurance Coverage 91
9.2.2 Other Assets 91
9.2.3 Insurance Or Warranty Coverage For End-Entities 91
9.2.4 Fiduciary Relationships 92
9.3 Confidentiality Of Business Information 92
9.3.1 Scope Of Confidential Information 92
9.3.2 Information Not Within The Scope Of Confidential Information 92
9.3.3 Responsibility To Protect Confidential Information 92
9.4 Privacy Of Personal Information 93
9.4.1 Privacy Plan 93
9.4.2 Information Treated As Private 93
9.4.3 Information Deemed Not Private 93
9.4.4 Responsibility To Protect Private Information 94
9.4.5 Notice And Consent To Use Private Information 94
9.4.6 Disclosure Pursuant To Judicial Or Administrative Process 94
9.4.7 Other Information Disclosure Circumstances 95
9.5 Intellectual Property Rights 95
9.5.1 Object Identifiers 95

9.5.2 Licences 95
9.5.3 IETF Guidelines 95
9.5.4 Breach 95
9.6 Representations And Warranties 96
9.6.1 Certification Authority Representations 96
9.6.2 Registration Authority Representations and Warranties 96
9.6.3 Certificate Holder Representations And Warranties 97
9.6.4 Relying Parties Representations And Warranties 98
9.6.5 Representations And Warranties Of Other Participants 99
9.7 Disclaimers Of Warranties 99
9.8 Liability and Limitations of Liability 99
9.8.1 QuoVadis Liability 99
9.8.2 QuoVadis' Limitations Of Liability 100
9.8.3 Excluded Liability 100
9.8.4 Mitigation Of QuoVadis' Liability 102
9.8.5 Claims Against QuoVadis Liability 103
9.9 Indemnities 103
9.10 Term And Termination 104
9.10.1 Term 104
9.10.2 Termination 104
9.10.3 Effect Of Termination And Survival 104
9.11 Individual Notices And Communications With Participants 104
9.12 Amendments 104
9.12.1 Procedure For Amendment 104
9.12.2 Notification Mechanism And Period 105
9.12.3 Circumstances Under Which Object Identifiers Must Be Changed 105
9.13 Dispute Resolution Provisions 106
9.14 Governing Law 106
9.15 Compliance With Applicable Law 107
9.16 Miscellaneous Provisions 107
9.16.1 Entire Agreement 107
9.16.2 Assignment 107
9.16.3 Severability 107
9.16.4 Enforcement (Attorneys' Fees And Waiver Of Rights) 107
9.16.5 Force Majeure 108
9.17 Other Provisions 108
10 APPENDIX A 109
10.1 Digital Certificate Profiles 109
10.1.1 QuoVadis Certificate Class 109
10.1.2 Key Usage and Archive 111
10.2 QV Standard 112

10.3 QV Advanced 113
10.4 QV Advanced + ... 115
10.4.1 ElDI-V/GeBüV Certificates 117
10.4.2 SuisseID Identity and Authentication Certificates 118
10.5 QV Qualified - eIDAS 121
10.5.1 eIDAS Qualified Certificate issued to a natural person on a QSCD 121
10.5.2 eIDAS Qualified Certificate issued to a natural person 123
10.5.3 eIDAS Qualified Certificate issued to a legal person on a QSCD 126
10.5.4 eIDAS Qualified Certificate issued to a legal person 129
10.6 QV Qualified - Legacy 132
10.6.1 Qualified Certificate Profile 132
10.6.2 Qualified Certificate Profile – Organisation / QCP Public 134
10.7 QV Qualified – SuisseID 136
10.8 QV Closed Community 138
10.8.1 Grid Certificates 138
10.9 QuoVadis Device 142
11 APPENDIX B 145
11.1 Business SSL 145
11.2 Code Signing 148
12 APPENDIX C 153
12.1.1 Definitions and Acronyms 153

1 Introduction

1.1 Overview

This QuoVadis CP/CPS sets out the policies, processes and procedures followed in the generation, issue, use and management of Key Pairs and Digital Certificates. It also describes the roles, responsibilities and relationships of Participants within the QuoVadis PKI.

This CP/CPS outlines the trustworthiness and integrity of the QuoVadis Root CAs' operations. A fundamental concept underpinning the operation of the QuoVadis PKI is trust. Trust must be realised in each and every aspect of the provision of Certification Services and Operations including Certificate Holder applications, issuance, renewal, revocation or expiry.

With the exception of Certification Authorities issuing Qualified Certificates in accordance with Swiss Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing CA and Registration Authority services within the QuoVadis PKI.

With the exception of Certification Authorities issuing Qualified Certificates in accordance with the European eIDAS Regulation, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing CA and Registration Authority services within the QuoVadis PKI.

Trust Service Provider component services for European Qualified Certificates may only be performed by QuoVadis approved entities that have the relevant certifications.

QuoVadis maintains several accreditations and certifications of its Public Key Infrastructure. These include:

- WebTrust for Certification Authorities and WebTrust SSL Baseline with Network Security conducted by Ernst & Young. These WebTrust audits are consistent with standards developed by the American National Standards Institute (ANSI), International Organisation for Standardization (ISO), and Internet Engineering Task Force (IETF). The WebTrust Principles and Criteria are consistent with the practices established by the CA/Browser Forum.
- Qualified Certification Service Provider (Switzerland) entitled to issue and administer Qualified Certificates, conducted by KPMG AG. This includes certification to ZertES, VZertES and TAV-ZertES, which are defined in section 8.1.1.

- Accredited Certification Authority by the EU Policy Management Authority for Grid Authentication in e-Science (EUGridPMA). This entitles QuoVadis to issue Digital Certificates meeting the guidelines of the International Grid Trust Federation (IGTF), which will enable validated and approved Grid users to gain access to Grid related resources.
- Accredited Certification Service Provider under PKIoverheid. PKIoverheid is the name for the PKI designed for trustworthy communication within and with the Dutch Government. Please note that there is a separate QuoVadis Certification Practice Statement (CPS) for PKIoverheid, which can be found in the QuoVadis Repository on the QuoVadis website (https://www.quovadisglobal.com).
- Authorised Certification Service Provider (Bermuda) entitled to issue Accredited Certificates under the requirements of the Electronic Transactions Act 1999. This authorisation synthesises elements of the ISO 17799 Code of Practice for Information Security Management and the European Electronic Signature Standardisation Initiative, as well as the WebTrust for Certification Authorities programme.

QuoVadis ensures the integrity of its 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. This CP/CPS merely provides a general overview of the QuoVadis PKI including Digital Certificate Profiles as defined in Appendix A and Appendix B.

The QuoVadis PKI is designed and is operated to comply with the broad strategic direction of existing international standards for the establishment and operation of a Public Key Infrastructure Certification Authority. Any person seeking to rely on Digital Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation.

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

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

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

QuoVadis ensures the integrity of its Public Key Infrastructure (PKI) operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between QuoVadis and any Participant in

the QuoVadis PKI. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation.

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

I. Business SSL Certificates are Certificates for which limited authentication and authorization checks are performed on the Certificate Holder and the individuals acting for the Certificate Holder.
II. Code Signing Certificates are Certificates issued in compliance with the Code Signing Minimum Requirements, including identification of the Certificate subject by a verified organization name and Certificate revocation for any misrepresentation or publication of malicious code.

QuoVadis Certificates comply with Internet standards (x509 v.3) as set out in RFC 5280 (which supersedes RFC 3280). This CP/CPS follows the IETF PKIX RFC 3647 framework with 9 sections that cover practices and procedures for identifying Certificate applicants; issuing and revoking Certificates; and the security controls related to managing the physical, personnel, technical, and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some sections will have the statement "Not applicable" or "No Stipulation."

Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS Regulation”) came into force on 1 July 2016. QuoVadis issues Qualified (and also non-Qualified) Certificates in accordance with the eIDAS Regulation. QuoVadis is listed on the Trusted List for the Netherlands (https://webgate.ec.europa.eu/tl-browser/#/trustmark/NL/NTRNL-30237459) and also the Trusted List for Belgium (https://webgate.ec.europa.eu/tl-browser/#/trustmark/BE/VATBE-0537698318).

This CP/CPS undergoes a regular review process and is subject to amendment on at least an annual basis as prescribed by the QuoVadis Policy Management Authority.

The structure of this CP/CPS is based on the RFC 3647 Certificate Policy and Certification Practices Framework, but does not seek to adhere to or follow it exactly.

Any and all references to a Certificate Policy within every aspect the QuoVadis PKI refers to policies contained in the current and in-force CP/CPS.

Where applicable, QuoVadis conforms to the current version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) published at http://www.cabforum.org, and the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates (“Code Signing Minimum Requirements”) published at https://aka.ms/csbr. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.2 Document Name, Identification and Applicability

The Private Enterprise Object Identifier (OID) assigned by the Internet Assigned Numbers Authority to QuoVadis is 1.3.6.1.4.1.8024.

The Object Identifiers assigned to the Root CAs covered by this CP/CPS are:

- QuoVadis Root Certification Authority/QuoVadis Root CA 1 G3 1.3.6.1.4.1.8024.0.1
- QuoVadis Root CA 3/QuoVadis Root CA 3 G3 1.3.6.1.4.1.8024.0.3

QuoVadis Root CA 2 is used to issue Extended Validation (EV) SSL Certificates associated with EV OID 1.3.6.1.4.1.8024.0.2.100.1.2, Business SSL Certificates and also Code Signing Certificates. Digital Certificates issued under Root CA 2 and QuoVadis Root CA 2 G3 have their own CP/CPS.

1.3 Public Key Infrastructure Participants

This CP/CPS outlines the roles and responsibilities of all parties involved in the generation and use of Digital Certificates and the operation of all QuoVadis-approved:

- Issuing CA services.
- Registration Authority services.

QuoVadis, in its capacity as the Certification Authority, holds the QuoVadis Root Certificates. The QuoVadis Root CA represents the apex of the QuoVadis PKI. The QuoVadis Root CA digitally creates, signs and issues Issuing CA Certificates using one of the Root Certificates identified above. Issuing CA Certificates are only issued to Approved Issuing CAs. An Approved Issuing CA utilises its Issuing CA Certificate to create, sign and issue Digital Certificates.

QuoVadis Issuing CAs are subordinate services that are:

- managed and operated by QuoVadis; or
- managed by third party Organisations but operated by QuoVadis (outsourced services).

Approved Client Issuing CAs are subordinate services that are managed and operated by clients (external services) and meet the contractual, audit and policy requirements of the QuoVadis CP/CPS with regard to operational practices and technical implementation.

Approved Registration Authorities act as the interface between Issuing CAs and an Applicant for a Digital Certificate. Approved RAs perform due diligence on potential Certificate Holders and only successful applicants are approved and receive Digital Certificates.

If you are not familiar with Common Terms usually employed in a PKI please refer to the Key Terms and Definitions in Appendix C.

QuoVadis provides identification and authentication services for Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this CP/CPS and in Appendix A and Appendix B define the credentials necessary to establish the identity of an individual or entity.

This CP/CPS describes all subordinate services that operate under the QuoVadis Root CA, i.e. that are within the QuoVadis "chain of trust".

Participants ("Participants") within the QuoVadis PKI include:

- Certification Authorities;
- Registration Authorities;
- Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance; and
- Authorised Relying Parties.

The practices described or referred to in this CP/CPS:

- accommodate the diversity of the community and the scope of applicability within the QuoVadis chain of trust; and
- adhere to the purpose of the CP/CPS of describing the uniformity and efficiency of practices throughout the QuoVadis PKI.

In keeping with their primary purpose, the practices described in this CP/CPS:

- are the minimum requirements necessary to ensure that Certificate Holders and Authorised Relying Parties have a high level of assurance, and that critical functions are provided at appropriate levels of trust; and
- apply to all stakeholders, for the generation, issue, use and management of all Digital Certificates and Key Pairs.

QuoVadis Digital Certificates comply with Internet Standards (x509 v.3) as set out in RFC 5280 (which supersedes RFC 3280).

Applications are as follows: secure electronic mail, retail transactions, IPSEC applications, secure TLS/SSL applications, contract-signing applications, custom e-Commerce applications and other certificate-enabled applications.

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

1.3.1 Certification Authorities

1.3.1.1 Root Certification Authority

The QuoVadis PKI contains the following Root Certificates:

SHA1 Roots	SHA256 Roots
QuoVadis Root Certification Authority	QuoVadis Root CA 1 G3
QuoVadis Root CA 2	QuoVadis Root CA 2 G3
QuoVadis Root CA 3	QuoVadis Root CA 3 G3

This CP/CPS relates to the QuoVadis Root Certification Authority, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3. QuoVadis Root CA 2 and QuoVadis Root CA 2 G3 have a separate CP/CPS.

The inclusion of the SSL OIDs (1.3.6.1.4.1.8024.0.1.100.1.1 and 1.3.6.1.4.1.8024.0.3.100.1.1) in the certificatePolicies extension of an end entity certificate asserts adherence to and compliance with the Baseline Requirements.

QuoVadis is obligated to operate the QuoVadis Root Certification Authority, QuoVadis Issuing CAs, and QuoVadis RAs in accordance with this QuoVadis CP/CPS and other relevant operational policies and procedures with respect to the issuance and management of Digital Certificates.

1.3.1.2 Issuing CAs and Their Obligations

Issuing CAs may be operated by QuoVadis or by other Organisations that have been authorised by QuoVadis to participate within the QuoVadis PKI to issue, revoke and otherwise manage Digital Certificates. Issuing CAs are required to act in accordance with their respective Issuing CA Agreements and to be bound by the terms of this

CP/CPS. Generally, Issuing CAs will be authorised to issue and manage all types of Digital Certificates supported by this CP/CPS.

For European Qualified Certificates issued out of the itsme Sign Issuing CA G1, the Registration Service and Subject Device Provisioning Service are not performed by QuoVadis. These services are performed entirely by Belgian Mobile ID, who undergo their 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 G1.

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 Policy Management Authority.

Within the QuoVadis PKI all Issuing CAs are responsible for the management of Digital Certificates issued by them. Digital Certificate Management includes all aspects associated with the application, issue and revocation of Digital Certificates, including any required identification and authentication processes included in the Digital Certificate application process. Issuing CAs, if authorised to do so by QuoVadis, may rely on third party Registration Authorities in the performance of Certificate Holder Identification and Authentication requirements. In circumstances where an Issuing CA has relied on a third party Registration Authority to perform Identification and Authentication, the Issuing CA bears all responsibility and liability for the Identification and Authentication of its Certificate Holders.

Notwithstanding the foregoing, Issuing CAs are required to conduct regular compliance audits of their Registration Authorities to ensure that they are complying with their obligations according to their respective RA Agreements, (including the performance of Identification and Authentication requirements) and this CP/CPS. Issuing CAs are required to ensure that all aspects of the services they offer and perform within the QuoVadis PKI are in compliance at all times with this CP/CPS.

Issuing CAs chaining to a QuoVadis Root must not be used for Man in the Middle (MITM) purposes for the interception of encrypted communications. Such Issuing CAs should also not be used for traffic management of domain names /IP addresses that the entity does not own or control. QuoVadis will not issue a subordinate Issuing CA Certificate to be used for these purposes.

Issuing CAs are required to ensure that;

- FIPS 140-3 or equivalent cryptographic modules are used for CA Private Key management.

- Private Keys are used only in connection with the signature of Digital Certificates and Certificate Revocation Lists.
- Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
- All administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CP/CPS.
- They comply at all times with all compliance audit requirements.
- They follow a privacy policy in accordance with this CP/CPS and applicable Issuing CA Agreement.

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

1.3.1.3 Approved Client Issuing CAs and Their Obligations

An Organisation wishing to participate in the QuoVadis PKI in the capacity of an Approved Client Issuing CA must supply to QuoVadis satisfactory evidence of that Organisation's ability to operate in accordance with the performance standards and other obligations that QuoVadis, in its sole discretion, requires of its Issuing CAs. Organisations wishing to act as Client Approved Issuing CAs will be required to enter into and act in accordance with an Issuing CA Agreement and this CP/CPS.

Approved Client Issuing CAs may not act as public or commercial CAs without the explicit approval of QuoVadis.

Execution of an Issuing CA Agreement is subject to review and acceptance by QuoVadis and/or QuoVadis auditors of a PKI infrastructure review that includes but is not limited to:

- CA hierarchy
- Logical, physical and network security measures
- Use of cryptographic modules

QuoVadis, in its sole discretion, may require one or all of the following:

- Independent audit of the Issuing CAs practices and operations and public attestation of conformance to this CP/CPS; or
- Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance; or

- Embedded technical constraints in the Issuing CA Certificate which may include the use of Path Length constraints, Extended Key Usage (EKU) extensions and/or Name Constraints; or
- Alternative technical constraints to restrict issuance of Digital Certificates in contravention of the Issuing CA Agreement.

Client Approved Issuing CAs must:

- Provide correct and accurate information in their communications with QuoVadis;
- Notify QuoVadis of material changes to their CA environment as defined in the PKI Infrastructure Review;
- Prevent compromise, loss, disclosure, modification or otherwise unauthorised use of their Private Key.
- Refrain from tampering with a QuoVadis CA Certificate;
- Cooperate with QuoVadis' own external auditors as required; and
- Cease to use the Issuing CA Certificate when it becomes invalid.

1.3.2 Registration Authorities and Their Obligations

Issuing CAs may, subject to the approval of QuoVadis, designate specific QuoVadis Registration Authorities to perform the Identification and Authentication and Digital Certificate request and revocation functions defined by this CP/CPS. All QuoVadis RAs are required to fulfil their functions and obligations in accordance with this QuoVadis CP/CPS and a Registration Authority Agreement to be entered into between the QuoVadis RA and the relevant Issuing CA.

QuoVadis RAs discharge their obligations in accordance with the practices outlined in this CP/CPS and the applicable Registration Authority Agreement.

Registration Authorities must perform certain functions in accordance with this CP/CPS and applicable Registration Authority Agreement which include but are not limited to;

- Process all Digital Certificate application requests;
- Maintain and process all supporting documentation related to Digital Certificate applications;
- Process all Digital Certificate Revocation requests;
- Comply with the provisions of its QuoVadis Registration Authority Agreement and the provisions of this QuoVadis CP/CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and
- Follow a privacy policy in accordance with this CP/CPS and the applicable Registration Authority Agreement.

QuoVadis acts as RA for all Certificates it issues in accordance with the Baseline Requirements. Third parties, who enter into a contractual relationship with QuoVadis, may act as Enterprise Registration Authorities (ERAs) and authorise the issuance of TLS/SSL Certificates by QuoVadis for Organisations and Domains that have been vetted by QuoVadis and pre-authenticated by QuoVadis. ERAs must abide by all the requirements of this CP/CPS and the terms of their services agreement with QuoVadis. ERAs may also implement more restrictive practices based on their internal requirements. QuoVadis does not delegate authority to third party RAs to vet TLS/SSL Certificate contents.

1.3.3 Certificate Holders

1.3.3.1 Obligations And Responsibilities

Certificate Holders are required to act in accordance with this CP/CPS and Certificate Holder Agreement. A Certificate Holder represents, warrants and covenants with and to QuoVadis, Relying Parties, Application Software Suppliers and the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A and Appendix B.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing CA, Registration Authority, or QuoVadis immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorised viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorised use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key. In the case of legal persons, the private key must be maintained and used under the control of the Certificate Holder and is recommended to be used only for electronic seals.
- Immediately notify the Issuing CA, Registration Authority or QuoVadis in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other

way whatsoever. Following compromise, the use of the Certificate Holder's Private Key should be immediately and permanently discontinued.

- Take all reasonable measures to avoid the compromise of the security or integrity of the QuoVadis PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.
- Discontinue the use of the digital signature Key Pair in the event that QuoVadis notifies the Certificate Holder that the QuoVadis PKI has been compromised.
- If the policy requires the use of a Qualified Electronic Signature Creation Device (QSCD), digital signatures must only be created by a QSCD.
- For Qualified certificates issued to natural persons, it is recommended that the Certificate Holder's key pair is only used for electronic signatures.

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

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

1.3.3.2 Accepted Limitation Of Liability

Digital Certificates include a reference to the relevant CP/CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Certificate Holders acknowledge and agree to all such limitations and disclaimers documented in the CP/CPS.

1.3.4 Relying Parties

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to become an “Authorised Relying Party” as defined in this CP/CPS, a Relying Party must exercise Reasonable Reliance as set out in this section 1.3.4.

All obligations within this section 1.3.4 relate to Reasonable Reliance on the validity of a Digital Signature, not the accuracy of the underlying electronic record.

This CP/CPS does not require a Certificate Holder to ensure that potential relying parties are compliant with the requirements to be an Authorised Relying Party.

1.3.4.1 Obligations and Responsibilities

Authorised Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement.

An Authorised Relying Party must utilise Digital Certificates and their corresponding Public Keys only for authorised and legal purposes and only in support of transactions or communications supported by the QuoVadis PKI.

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance and that Authorised Relying Party is otherwise in compliance with the terms and conditions of their Relying Party Agreement. Any such Reliance is made solely at the risk of the Relying Party.

1.3.4.2 Reasonable Reliance

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance (as set out below) and that Authorised Relying Party is otherwise in compliance with the terms and conditions of the Authorised Relying Party Agreement and this CP/CPS. For the purposes of this CP/CPS and Relying Party Agreement, the term "Reasonable Reliance" means:

- that the attributes of the Digital Certificate relied upon are appropriate in all respects to the reliance placed upon that Digital Certificate by the Authorised Relying Party including, without limitation to the generality of the foregoing, the level of Identification and Authentication required in connection with the issue of the Digital Certificate relied upon;
- that the Authorised Relying Party has, at the time of that reliance, used the Digital Certificate for purposes appropriate and permitted under this QuoVadis CP/CPS;
- that the Authorised 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 Authorised Relying Party;
- that the Digital Certificate intended to be relied upon is valid and has not been revoked, the Authorised Relying Party being obliged to check the status of that Digital Certificate utilising either the QuoVadis Database, the QuoVadis Certificate Revocation List, or the QuoVadis Online Certificate Status Protocol and otherwise in accordance with the provisions of this QuoVadis CP/CPS;
- that the Authorised Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- that the Authorised Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Digital Certificate being relied upon;
- that the Authorised Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software;
- that the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
- that the identity of the Certificate Holder is displayed correctly by utilising trusted application software; and
- that any alterations arising from security changes are identified by utilising trusted application software.

1.3.4.3 Accepted Limitation Of Liability

Digital Certificates include a reference to the relevant CP/CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers documented in the CP/CPS.

1.3.4.4 Assumptions About A Certificate Holder

A relying party shall make no assumptions about information that does not appear in a Digital Certificate.

1.3.4.5 Certificate Compromise

A party cannot rely on a Digital Certificate issued by QuoVadis if the party has actual or constructive notice of the compromise of the Digital Certificate or its associated Private Key. Such notice includes but is not limited to the contents of the Digital Certificate and information incorporated in the Digital Certificate by reference, which includes this CP/CPS and the current set of revoked Digital Certificates published by QuoVadis. Certificates have pointers to URLs where QuoVadis publishes status information, including Certificate Revocation Lists (CRLs), and Relying Parties are required to check the most recent CRL.

1.3.5 Other Participants

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant QuoVadis documentation. All application software and operating system vendors with whom QuoVadis has entered into a contract for inclusion of the QuoVadis Root Certificate as a trusted trust anchor in their software are intended third party participants in the QuoVadis PKI.

1.4 Certificate Usage

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

1.4.1 Appropriate Certificate Usage

Digital Certificates may be used for identification, providing data confidentiality and data integrity, and for creating digital signatures.

The use of Digital Certificates supported by this CP/CPS is restricted to parties authorised by contract to do so. Persons and entities other than those authorised by contract may not use Digital Certificates for any purpose. No reliance may be placed on a Digital Certificate by any Person unless that Person is an Authorised Relying Party.

A Digital Certificate does not convey evidence of authority of an Individual to act on behalf of any person or to undertake any particular act, and Authorised Relying Parties are solely responsible for exercising due diligence and reasonable judgement before choosing to place any reliance whatsoever on a Digital Certificate. A Digital Certificate is not a grant, assurance, or confirmation from QuoVadis of any authority, rights, or privilege save as expressly set out in this CP/CPS or expressly set out in the Digital Certificate.

Any person participating within the QuoVadis PKI irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this CP/CPS shall occur and shall be deemed to occur in Bermuda and that the

performance of QuoVadis' obligations hereunder shall be performed and be deemed to be performed in Bermuda.

1.4.2 Prohibited Certificate Usage

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

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

1.5 Policy Administration

1.5.1 Organisation Administering the CP/CPS

QuoVadis operates the Policy Management Authority (PMA) that is responsible for setting policies and practices for the overall PKI.

1.5.2 Contact Person

This CP/CPS is administered by the QuoVadis PMA. Enquiries or other communications about this CP/CPS should be addressed to QuoVadis Limited.

Policy Director
QuoVadis Limited
Suite 1640,
48 Par-La-Ville Road,
Hamilton HM-11, Bermuda

Website: https://www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

1.5.3 Person Determining the CP/CPS Suitability

The QuoVadis PMA determines the suitability of this CP/CPS to the functions and uses of Participants in the QuoVadis PKI.

1.5.4 CP/CPS Approval Procedures

This CP/CPS is regularly reviewed and approved by the QuoVadis PMA. Notice of proposed changes are recorded in the change log at the beginning of this CP/CPS until they are approved, at which time the approved change will be recorded there

permanently. 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.

1.5.4.1 Publication of CP/CPS

This CP/CPS is published electronically in PDF format at https://www.quovadisglobal.com/repository.

1.5.4.2 Frequency of Publication

Newly approved versions of this CP/CPS, Certificate Holder or Relying Party Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those documents. Information about amendments to this CP/CPS may be found in Section 9.12.

1.5.4.3 Access Control

QuoVadis internal documents not published at https://www.quovadisglobal.com/repository are available only to Participants in the QuoVadis PKI where deemed necessary.

1.6 Definitions and Acronyms

See Appendix C.

2 Publication and Repository Responsibilities

2.1 Repositories

The QuoVadis Repository (https://www.quovadisglobal.com/repository) serves as the primary repository. However, copies of the X.500 Directory may be published at such other locations as are required for the efficient operation of the QuoVadis PKI.

2.2 Publication of Certificate Information

The QuoVadis Root Certification Authority and chained Issuing CAs publish a Repository that lists all Digital Certificates issued and all the Digital Certificates that have been revoked. The location of the repository and Online Certificate Status Protocol responders are given in the individual Certificate Profiles more fully disclosed in Appendix A and Appendix B to this CP/CPS.

QuoVadis Root, Issuing CA and Time-Stamp certificates are published at https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx.

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

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

2.3 Time or Frequency of Publication

Digital Certificate information is published promptly following generation and issue and immediately following the completion of the revocation process.

2.4 Access Controls on Repositories

Read-only access to Repositories is available to Relying Parties twenty-four hours per day, seven days per week, except for reasonable maintenance requirements, where access is deemed necessary. Queries to the Repository must specify individual Certificate information. QuoVadis is the only entity that has write access to Repositories.

3 Identification and Authentication

QuoVadis implements rigorous authentication requirements to ensure that the identity of the Certificate Holder is proven. This may include face-to-face identity verification at the beginning of the Digital Certificate request procedure or at some point prior to Digital Certificate delivery to the Certificate Holder. The registration procedure will depend on the class and type of Digital Certificate that is being applied for.

Issuing CAs may perform the Identification and Authentication required in connection with the issue of Digital Certificates, or they may delegate the responsibility to one or more Registration Authorities. The level of Identification and Authentication depends on the class (QuoVadis Certificate Class) of Digital Certificate being issued (See Appendix A and Appendix B).

3.1 Naming

3.1.1 Types Of Names

All Certificate Holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The QuoVadis Root Certification Authority approves naming conventions for the creation of distinguished names for Issuing CA applicants. Different naming conventions may be used by different Issuing CAs.

The Subject Name of all Digital Certificates issued to Individuals shall be the authenticated common name of the Certificate Holder. Each User must have a unique and readily identifiable X.501 Distinguished Name (DN). The Distinguished Name may include the following fields:

- Common Name (CN)
- Organisational Unit (OU)
- Organisation (O)
- Locality (L)
- State or Province (S)
- Country (C)
- Email Address (E)

Alternatively, Distinguished Names 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 Digital Certificates covered under the Baseline Requirements, 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 the Subject Alternative Name extension.

TLS/SSL Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service, or application that has been confirmed with the Certificate Holder. The Distinguished Names of a Code Signing Certificate must identify the legal entity that intends to have control over the use of the Private Key when signing code. The Baseline Requirements contain provisions prohibiting Certificates containing Internal Server Names or Reserved IP Addresses.

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

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

3.1.2 Need For Names To Be Meaningful

Distinguished Names must be meaningful and unambiguous. QuoVadis supports the use of Digital Certificates as a form of identification within a particular community of interest.

The contents of the Digital Certificate Subject Name fields must have a meaningful association with the name of the Individual, Organisation, or Device. In the case of Individuals, the name should consist of the first name, last name, and any middle initial. In the case of Organisations, the name shall meaningfully reflect the legal name or registered domain name of the Organisation or the trading or business name of that Organisation. In the case of a Device, the name shall state the name of the Device and the legal name or registered domain name of the Organisation responsible for that Device.

3.1.3 Pseudonymous Certificate Holders

Pseudonym Digital Certificates may only be issued if permitted for that class/type of Digital Certificates and only in accordance with relevant industry standards.

3.1.4 Rules For Interpreting Various Name Forms

Fields contained in Digital Certificates are in compliance with this CP/CPS and the Digital Certificate Profiles detailed in Appendix A. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5 Uniqueness Of Names

QuoVadis Registration Authorities propose and approve distinguished names for Applicants, and, as a minimum check that a proposed distinguished name is unique, verify that the name is not already listed in the QuoVadis X.500 Directory.

The Subject Name of each Digital Certificate issued by an Issuing CA shall be unique within each class of Digital Certificate issued by that Issuing CA and shall conform to all applicable X.500 standards for the uniqueness of names. The Issuing CA may, if necessary, insert additional numbers or letters to the Certificate Holder's Subject Common Name, or other attribute such as subject serialNumber, in order to distinguish between two Digital Certificates that would otherwise have the same Subject Name.

3.1.6 Recognition, Authentication, And Role Of Trademarks

Issuing CAs are not obligated to seek evidence of trademark usage by any Organisation.

3.2 Initial Identity Validation

Identity Validation of individual Certificate Holders is in compliance with this CP/CPS and the Digital Certificate Profiles detailed in Appendix A and Appendix B.

3.2.1 Method To Prove Possession Of Private Key

Issuing CAs shall establish that each Applicant for a Digital Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the request for a Digital 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 Certificate Holder.

3.2.2 Authentication Of Organisation Identity

The Identity of an Organisation is required to be authenticated with respect to each Digital Certificate that asserts (i) the identity of an Organisation; or (ii) an Individual or Device's affiliation with an Organisation. Without limitation to the generality of the foregoing, the Identity of any Organisation that seeks to act as a Registration Authority 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, at a minimum, confirmation is required that: (i) the Organisation legally exists in the name that will appear in the Distinguished Name of any Digital 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 Digital 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. 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 Registration Authority has a separate and pre-existing commercial relationship with the Organisation under review, the Issuing CA or Registration Authority 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 Registration Authority shall record the specific records upon which it relied for this purpose.

With respect to TLS/SSL certificates, authentication of Organisation identity is conducted in compliance with this CP/CPS and the SSL Certificate Profiles detailed in Appendix B.

3.2.2.1 Validation of Domain Authorization and Control

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

1. Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation)
2. Communicating directly with the Domain Name Registrant by calling their phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The phone number used must be the number listed by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.3;
3. Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorization Domain Name. Performed in accordance with BR section 3.2.2.4.4;
4. Confirming the Applicant's control over the requested FQDN by confirming the presence of an agreed-upon Random Value under the "/.well-known/pki-validation" directory. Performed in accordance with BR section 3.2.2.4.6;
5. Confirming the Applicant's control over the requested Authorization Domain Name (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value in a DNS record. Performed in accordance with BR section 3.2.2.4.7;
6. Confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8;
7. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12;
8. Confirming the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact and then receiving a confirming response utilizing the Random Value. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13;

9. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14;
10. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; and
11. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.

High Risk Domains

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

3.2.2.2 Authentication for an IP Address

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

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

Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;

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

After July 31, 2019, QuoVadis will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;

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

Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or

Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

3.2.2.3 Wildcard Domain Validation

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

3.2.2.4 Data Source Accuracy

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

3.2.3 Authentication Of Individual Identity

An Individual's Identity is to be authenticated in accordance with the class/type of Digital Certificate together with the relevant application data and documentation. TLS/SSL Certificates are only issued to organisations and not natural persons.

3.2.4 Non-Verified Certificate Holder Information

The QuoVadis Issuing CA may accept any form of Non-Verified Holder Information for the issuance of Digital Certificates used solely for demonstration or testing purposes.

An Issuing CA within the QuoVadis PKI may accept the following Non-Verified Certificate Holder Information for other classes of Digital Certificate:

- Organisational Unit (OU)
- Other information that is permitted as Non-Verified according to the Certificate class or relevant industry standards

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 Registration Authority will validate the Applicant's Authority by reference to business records maintained by the Registration Authority, its Subsidiaries, Holding Companies or Affiliates. Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

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 Renewal Requests

QuoVadis does not support Certificate Renewal. Key Pairs must always expire at the same time as the associated Digital Certificate. Certificate Renewal requests are treated in the same manner as an initial Certificate Request and a new Digital Certificate and new Key Pair is issued. Application for a Digital Certificate following revocation is treated as though the person requesting the replacement were a new Applicant.

3.3.1 Identification and Authentication For Routine Re-Key

Identification and Authentication for routine Re-Key is based on the same requirements as issuance of new Certificates.

3.3.2 Identification and Authentication For Re-Key After Revocation

Identification and Authentication for Re-Key after revocation is based on the same requirements as issuance of new Certificates.

3.4 Identification and Authentication For Revocation Requests

A request to revoke Keys and Digital Certificates may be submitted by persons authorised to do so under relevant contractual documentation.

3.4.1 Issuing Certification Authority

An authorised individual acting under the authority of the Issuing CA may revoke a Digital Certificate by communicating with the QuoVadis Digital Certificate administration system using a QV Utility Digital Certificate.

3.4.2 Registration Authority

A Registration Authority may request the revocation of Digital Certificates it has caused to be issued by requesting, in person, by digitally signed electronic mail or by authenticating to the QuoVadis Digital Certificate administration system that an authorised member of the Issuing CA staff revoke the Digital Certificate/s in question.

3.4.3 Certificate Holder

A Certificate Holder may request that his or her Digital Certificate be revoked by:

- Authenticating to the QuoVadis Digital Certificate administration system or other relevant system and requesting revocation via this system;
- Applying in person to the Registration Authority, Issuing CA or QuoVadis supplying either original proof of identification in the form of a valid Driving License or Passport;
- Sending a digitally signed email message to the Issuing Registration Authority, Issuing CA or QuoVadis requesting that their Digital Certificate be revoked.
- Telephonic communication using a pre-existing shared secret, password or other information associated with Certificate Holder's account with the Certification Authority following appropriate Identification.

4 Certificate Life-Cycle Operation Requirements

4.1 Certificate Application

Digital Certificate applications are subject to various assessment procedures depending upon the type of Digital Certificate applied for.

4.1.1 Who Can Submit A Certificate Application

An application in a form prescribed by the Issuing CA must be completed by Applicants, which includes all registration information as described by this CP/CPS (including, without limitation, that information set out in Appendix A) and the relevant Certificate Holder Agreement or other terms and conditions upon which the Digital Certificate is to be issued. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

4.1.2 Enrolment Process And Responsibilities

Certain information concerning applications for Digital Certificates is set out in this QuoVadis CP/CPS. However, the issue of Digital Certificates by Issuing CAs will be pursuant to forms and documentation required by that Issuing CA. Notwithstanding the foregoing, the following steps are required in any application for a Digital Certificate: (i) Identity of the Holder or Device is to be established in accordance with Appendix A, (ii) a Key Pair for the Digital Certificate is to be generated in a secure fashion, (iii) the binding of the Key Pair to the Digital Certificate shall occur as set forth in this CP/CPS, and (iv) the Issuing CA shall enter into contractual relations with the Certificate Holder for the use of that Digital Certificate and the QuoVadis PKI.

Where Certificates are to be used for digitally signing and/or encrypting email messages, QuoVadis takes reasonable measures to verify that the entity submitting the request controls the email account referenced in the Certificate, or has a legal right to request a Certificate including the email address. QuoVadis systems perform a challenge-response procedure by sending an email to the email address to be included in the Certificate. The Applicant must respond with a shared secret within a limited time to demonstrate that they have control over that email address.

Each Issuing CA may adopt its own application forms and procedures, which Applicants will be required to satisfy. Each Holder of a Digital Certificate is required to be bound by contract with respect to the use of that Digital Certificate. These contracts may be directly between the Issuing CA and the Holder or imposed upon that Holder through terms and conditions binding upon him or her. All agreements concerning the use of, or

reliance upon, Digital 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

See Appendix A and Appendix B for Identification and Authentication requirements for each Digital Certificate profile.

4.2.2 Approval Or Rejection Of Certificate Applications

A Registration Authority will approve or reject Certificate Holder applications based upon the Certificate Holders meeting the requirements of this CP/CPS and the Digital Certificate Profiles contained in Appendix A.

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

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

QuoVadis, at its sole discretion not to be unreasonably withheld, may override any decision to Approve a Certificate Holder Application.

4.2.3 Time To Process Certificate Applications

Registration Authorities and Issuing CAs operating within the QuoVadis PKI are under no obligation to process Digital Certificate Applications other than within a commercially reasonable time.

4.2.4 Certificate Authority Authorisation (CAA)

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

When processing CAA records, QuoVadis processes the issue, issuewild, and iodef property tags as specified in RFC 6844 as amended by Errata 5065 (Appendix A).

QuoVadis may not act on the contents of the iodef property tag. QuoVadis will not issue a Digital Certificate if an unrecognized property is found with the critical flag.

QuoVadis may not check CAA records for the following exceptions:

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

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

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

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

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

4.3 Certificate Issuance

4.3.1 Certification Authority Actions During Certificate Issuance

Digital Certificate issuance is governed by and should comply with the practices described in and any requirements imposed by the QuoVadis CP/CPS.

4.3.1.1 QuoVadis Root Certification Authority

The Root Certification Authority Certificate has been self-generated and self-signed.

4.3.1.2 QuoVadis Issuing Certification Authority Certificates

Upon accepting the terms and conditions of the QuoVadis Issuing CA Agreement by the Issuing CA, successful completion of the Issuing CA application process as prescribed by QuoVadis, and final approval of the application by the QuoVadis Root Certification Authority, the QuoVadis Root Certification Authority issues the Issuing CA Digital Certificate to the relevant Issuing CA.

4.3.1.3 QuoVadis Registration Authority Appointment

Upon accepting the terms and conditions of the QuoVadis Registration Authority Agreement, successful completion of the Registration Authority application process and final approval of the application, the Registration Authority becomes duly appointed, and appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

4.3.1.4 Registration Authority Officer's Certificate

As part of the application process, Registration Authorities are required to nominate one or more persons within their Organisation to take responsibility for the operation their Registration Authority functions. Those nominated persons will each be issued a Registration Authority Officer's Digital Certificate.

4.3.1.5 Certificate Holder Certificates

Upon the Applicant's acceptance of the terms and conditions of the Certificate Holder Agreement or other relevant agreement, the successful completion of the application process and final approval of the application by the Issuing CA, the Issuing CA issues the Digital Certificate to the Applicant or Device.

4.3.2 Notification To Applicant Certificate Holder By The Certification Authority Of Issuance Of Certificate

Issuing CAs and Registration Authorities within the QuoVadis PKI may choose to notify Applicants that their Digital Certificate has been issued.

4.4 Certificate Acceptance

Digital Certificate acceptance is governed by and should comply with the practices described in, and any requirements imposed by, this CP/CPS.

Until a Digital Certificate is accepted, it is not published in any Repository or otherwise made publicly available. By using a Digital Certificate, the Holder thereof certifies and agrees to the statements contained in the notice of approval. This CP/CPS sets out what constitutes acceptance of a Digital Certificate. An Applicant that accepts a Digital Certificate warrants to the relevant Issuing CA, and all Authorised Relying Parties who reasonably rely, that all information supplied in connection with the application process and all information included in the Digital Certificate issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a Digital Certificate or the reliance upon a Digital Certificate signifies acceptance by that person of the terms and conditions of this QuoVadis CP/CPS and Certificate Holder Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

By accepting a Digital Certificate issued by an Issuing CA operating within the QuoVadis PKI, the Certificate Holder expressly represents and warrants to QuoVadis and all Authorised Relying Parties who reasonably rely on the information contained in the Digital Certificate that at the time of acceptance and throughout the operational period of the Digital Certificate, until notified otherwise by the Certificate Holder, that:

- No unauthorised person has ever had access to the Certificate Holder's Private Key;
- All representations made by the Certificate Holder to QuoVadis regarding the information contained in the Digital Certificate are true;
- All information contained in the Digital Certificate is true to the extent that the Certificate Holder had knowledge or notice of such information, and does not promptly notify QuoVadis of any material inaccuracies in such information; and
- The Digital Certificate is being used exclusively for authorised and legal purposes, consistent with this CP/CPS.

4.4.1 Notice Of Acceptance

BY ACCEPTING A DIGITAL CERTIFICATE, THE CERTIFICATE HOLDER ACKNOWLEDGES THAT HE OR SHE AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CERTIFICATE POLICY & CERTIFICATION PRACTICE STATEMENT AND THE APPLICABLE CERTIFICATE HOLDER AGREEMENT. ALSO BY ACCEPTING A DIGITAL CERTIFICATE, THE CERTIFICATE HOLDER ASSUMES A DUTY TO RETAIN CONTROL OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY CONTAINED IN THE CERTIFICATE, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT THE PRIVATE KEY'S LOSS, EXCLUSION, MODIFICATION, OR UNAUTHORISED USE.

4.4.2 Conduct Constituting Certificate Acceptance

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

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

The downloading, installing or otherwise taking delivery of a Digital Certificate constitutes acceptance of a Digital Certificate within the QuoVadis PKI.

4.4.3 Publication Of The Certificate By The Certification Authority

All Digital Certificates issued within the QuoVadis PKI are made available in public repositories, except where Certificate Holders have requested that their Digital Certificates not be published.

4.4.4 Notification Of Certificate Issuance By The Certification Authority To Other Entities

Issuing CAs and Registration Authorities within the QuoVadis PKI may choose to notify other Entities of Digital Certificate Issuance.

4.5 Key Pair And Certificate Usage

4.5.1 Certificate Holder Private Key And Certificate Usage

Within the QuoVadis PKI, a Certificate Holder may only use the Private Key and corresponding Public Key in the Digital Certificate for their lawful and intended use. The Certificate Holder accepts the Certificate Holder Agreement by accepting the Digital Certificate, and by accepting the Digital Certificate unconditionally agrees to use the Digital Certificate in a manner consistent with the Key-Usage field extensions included in the Digital Certificate Profile.

4.5.2 Relying Party Public Key And Certificate Usage

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to be an Authorised Relying Party, a Party seeking to rely on a Digital Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement (https://www.quovadisglobal.com/repository) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

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

- The appropriateness of the use of the Digital Certificate for any given purpose and that the use is not prohibited by this CP/CPS.
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.

- That the Digital Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

4.6 Certificate Renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key. The QuoVadis PKI does not support Certificate Renewal for end entity (non-CA) certificates.

QuoVadis does support renewal for Issuing CA Certificates.

4.7 Certificate Re-Key

Certificate Re-Key is when all the identifying information from a Digital Certificate is duplicated in a new Digital Certificate, but there is a different public key and a different validity period. Due diligence, Key Pair generation, delivery and management are performed in accordance with this CP/CPS.

4.7.1 Circumstance For Certificate Re-Key

Digital Certificates may be Re-Keyed upon request.

4.7.2 Who May Request Re-Key

Certificate Holders and Nominating Registration Authorities may request Digital Certificate Re-Keys.

4.7.3 Processing Certificate Re-Key Request

Digital Certificate Re-Key requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS. In order to process a Re-Key request, the Certificate Holder is required to confirm that:

- Details contained in the original Digital Certificate application have not changed.
- Authenticate their identity to the Registration Authority.

Using their existing Digital Certificate, the Certificate Holder may digitally sign an electronic message to the Nominating Registration Authority requesting that the Digital Certificate be Re-Keyed and confirming that the original application details have not changed. Appropriate vetting will be performed in relation to the details to be included in the Digital Certificate.

4.7.4 Notification Of New Certificate Issuance To Certificate Holder

Issuing CAs and Registration Authorities within the QuoVadis PKI shall notify Certificate Holders of Digital Certificate Issuance.

4.7.5 Conduct Constituting Acceptance Of A Re-Key Certificate

Downloading, installing or otherwise taking delivery of a Re-Keyed Digital Certificate constitutes acceptance of the Digital Certificate Re-Key within the QuoVadis PKI.

4.7.5.1 Publication Of The Re-Key Certificate By The Certification Authority

All Digital Certificate Re-Keys issued within the QuoVadis PKI are made available in public repositories except where Certificate Holders have requested that their Digital Certificates not be published.

4.7.6 Notification Of Certificate Re-Key By The Certification Authority To Other Entities

Issuing CAs and Registration Authorities within the QuoVadis PKI may choose to notify other entities of Digital Certificate Re-Key.

4.8 Certificate Modification

Certificate Modification refers to the issuance of a new Digital Certificate due to changes in the information in an existing Digital Certificate (other than its associated Public Key). QuoVadis may reissue or replace a valid Certificate when the Certificate Holder's common name, organization name, device name, or geographic location changes. Modified information must undergo the same Identification and Authentication procedures as for a new Certificate.

Digital Certificate Modification requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS.

4.9 Certificate Revocation And Suspension

4.9.1 Circumstances For Revocation

Digital Certificates shall be revoked when any of the information on a Digital Certificate changes or becomes obsolete or when the Private Key associated with the Digital Certificate is compromised or suspected to be compromised. A Digital Certificate will be revoked in the following instances upon notification of:

- QuoVadis Certification Authority key compromise
- Certificate Holder profile creation error

- Key Compromise including unauthorised access or suspected unauthorised access to Private Keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new Certificate.
- The Certificate Holder has failed to meet his, her or its obligations under this QuoVadis CP/CPS or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;
- The Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the Certificate Holder provided inaccurate, false or misleading information;
- The Private Key corresponding to the Certificate has been used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a user's system without their consent;
- The Certificate Holder is a denied party or prohibited person on a government-issued blacklist, or is operating from a prohibited destination;
- Where a Certificate Holder's employer or company that operates the Nominating Registration Authority, or its respective Subsidiaries, Holding Companies or Counterparties requests revocation because:
  - Of a change in the employment relationship with the Certificate Holder
  - The Certificate Holder is no longer authorised to act on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
  - The Certificate Holder otherwise becomes unsuitable or unauthorised to hold a Digital Certificate on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
- Affiliation change
- Cessation of operation
- Incorrect information contained in Digital Certificate
- Certificate Holder bankruptcy
- Certificate Holder liquidation
- Certificate Holder death
- Certificate Holder request
- Issuing Registration Authority Request
- Breach of Certificate Holder agreement with QuoVadis

- QuoVadis determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Certificate Holder requests in writing the revocation of their Certificate;
- The Certificate Holder indicates that the original Certificate Request was not authorised and does not retroactively grant authorization;
- QuoVadis obtains reasonable evidence that there has been loss, theft, modification, unauthorised disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate, or that the Certificate has otherwise been misused;
- QuoVadis receives notice or otherwise becomes aware that a Certificate Holder has breached a material obligation under the Certificate Holder Agreement or other contractual obligations;
- QuoVadis receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
- QuoVadis is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- QuoVadis is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- QuoVadis determines, in its sole discretion, that the Certificate was not issued in accordance with the terms and
- conditions of the EV Guidelines or QuoVadis' CP/CPS;
- QuoVadis receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Certificate Holder that is contained within the Certificate;
- The Certificate Holder fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;
- QuoVadis determines, in its sole discretion, that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
- If QuoVadis receives notice or otherwise becomes aware that a Certificate Holder has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination;

- Either the Certificate Holder's or QuoVadis' obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- A QuoVadis CA Private Key used to issue that Certificate has been compromised;
- Revocation is required by the QuoVadis CP/CPS
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
- QuoVadis' right to issue and manage Certificates under the EV Guidelines, the Baseline Requirements, or the Code Signing Minimum Requirements expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository); or
- QuoVadis ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

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

4.9.2 Who Can Request Revocation

The following entities may request revocation of a Digital Certificate:

- QuoVadis may revoke any Digital Certificate issued within the QuoVadis PKI at its sole discretion, and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.
- An Issuing CA operating within the QuoVadis PKI may revoke Digital Certificates that it has issued.
- A Registration Authority or Subscriber operating within the QuoVadis PKI may request revocation of Digital Certificates that it requested to be issued.
- Certificate Holders within the QuoVadis PKI may request revocation of their own Digital Certificates.
- An Application Software Vendor who has embedded a QuoVadis Root Certification Authority Certificate in its application as a trusted root may request the revocation of Digital Certificate chained to that Root Certificate.

4.9.3 Procedure For Revocation Request

QuoVadis will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the Issuing CA and the Registration Authority that approved or acted in connection with the issue thereof. The Certificate Holder may be required to submit the revocation request via the QuoVadis Support Line or directly over an Internet connection. The QuoVadis website (https://www.quovadisglobal.com) provides a mechanism in which to submit revocation requests. The Certificate Holder, Registration Authority or Issuing CA may be required to provide a shared secret or pass phrase that will be used to activate the revocation process. Digital Certificate revocation requests may also be issued by contacting the administrators of the Issuing CA or Registration Authority directly. A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Holder requesting revocation (or the Organisation, where applicable). Alternatively, the Holder (or Organisation, where applicable) may request revocation by contacting the Issuing CA and providing adequate proof of identification in accordance with this QuoVadis CP/CPS or an equivalent method.

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

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

For certificates issued from the itsme sign Issuing CA G1 all revocation requests must be directed to the itsme first-line helpdesk.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which The Certification Authority Must Process The Revocation Request

QuoVadis will begin investigation of a certificate problem report within 24 hours of its receipt. 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 G1 this 24 hour time period starts with the receipt of the revocation request at the itsme first-line helpdesk.

4.9.6 Revocation Checking Requirement For Relying Parties

Digital Certificate revocation information is provided via the Certificate Revocation List in the QuoVadis X.500 Directory services.

4.9.7 Certificate Revocation List Issuance Frequency

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

4.9.8 Maximum Latency For Certificate Revocation List

The maximum latency for the Certificate Revocation list is 10 minutes.

4.9.9 On-Line Revocation/Status Checking Availability

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

4.9.10 On-Line Revocation Checking Requirement

The validity of a QuoVadis Digital Certificate must be checked online using the QuoVadis Repository, the appropriate Certificate Revocation List or using the appropriate Online Certificate Status Protocol responder by a Relying Party seeking to become an Authorised Relying Party.

Failure to do so negates the ability of the Authorised Relying Party to claim that it acted on the Digital Certificate with Reasonable Reliance.

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

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

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements in Relation to Key Compromise

Should a Private Key become compromised, the related Certificate shall immediately be revoked. Should the private CA key become compromised, all Certificates issued by that CA shall be revoked.

4.9.13 Circumstances For Suspension

No suspension of Digital Certificates is permissible within the QuoVadis PKI.

4.9.14 Who Can Request Suspension

No suspension of Digital Certificates is permissible within the QuoVadis PKI.

4.9.15 Procedure For Suspension Request

No suspension of Digital Certificates is permissible within the QuoVadis PKI.

4.9.16 Limits On Suspension Period

No suspension of Digital Certificates is permissible within the QuoVadis PKI.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List (http://crl.quovadisglobal.com/<caname>.crl) or is made available via Online Certificate Status Protocol checking (http://ocsp.quovadisglobal.com) where available.

Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked certificate.

4.10.2 Service Availability

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

4.10.3 Optional Features

Online Certificate Status Protocol is available for all Certificate types issued by QuoVadis Issuing CAs.

4.11 End Of Subscription

Within the QuoVadis PKI a Certificate Holder may end a subscription by:

- Allowing a Digital Certificate to expire.
- Revoking a Digital Certificate.

4.12 Key Archival And Recovery

QuoVadis provides optional Key Archive services for certain Certificate Profiles (see Appendix A, section 10.1.2). Key archive is prohibited for QV Advanced+ and QV Qualified Certificates, or for any Private Key whose Key Usage is dedicated to Signing or Authentication. With respect to TLS/SSL and Codesigning certificates.The QuoVadis PKI does not support key escrow or recovery of Certificate Holder private keys.

4.12.1 Key Archival And Recovery Policy And Practices

Registration Authorities are permitted to instruct QuoVadis to archive the Certificate Holder's Private Key for certain Certificate Profiles as specified in their Registration Authority Agreement. End-user Certificate Holder Private Keys shall only be recovered under the circumstances permitted within the Registration Authority Agreement and Trust/Link Administrator Guide.

Archived Private Keys are stored in encrypted form using the QuoVadis Trust/Link application. Certificate Holders are notified when their Private Keys are archived.

Properly authenticated Certificate Holders may subsequently retrieve their own Private Keys.

In addition, properly authenticated RA Officers with specific Key Recovery permissions may request retrieval of a Certificate Holder's Private Keys under the following conditions:

- RAs must protect Certificate Holder's archived Private Keys from unauthorized disclosure.
- RAs may retrieve Certificate Holder's archived Private Keys only for properly authenticated and authorized requests for recovery.
- RAs shall recover a Certificate Holder's archived Private Keys without the Subscriber's authority only for legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose.
- RAs must revoke the Certificate Holder's Key Pair prior to recovering the Private Key.
- RAs may not disclose or allow to be disclosed archived keys or archive key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organisation policy; or by order of a court of competent jurisdiction.

- RAs are not required to communicate any information concerning a key recovery to the Certificate Holder except when the Certificate Holder has requested recovery.

4.12.2 Session Key Encapsulation And Recovery Policy And Practices

Not Stipulated.

5 Facility, Management, And Operational Controls

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

I. Protect the confidentiality, integrity, and availability of data and business process;
II. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of data and business process;
III. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of data and business process;
IV. Protect against accidental loss or destruction of, or damage to data and business processes; and
V. Comply with all other security requirements applicable to the CA by law and industry best practices.

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

5.1 Physical Controls

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

5.1.1 Site Location and construction

QuoVadis performs its CA operations from a secure datacentre located in Hamilton, Bermuda. The datacentre is a purpose-built steel and composite compartment, with raised floor construction and an array of resilient security and environmental systems. QuoVadis operates under a security policy designed to deter, prevent and detect unauthorized access to the datacentre.

5.1.2 Physical Access

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

5.1.3 Power and Air-Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Paper documents and magnetic media containing trusted elements of QuoVadis or commercially sensitive or confidential information are securely disposed of by:

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

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 24 hours per day seven days per week for the purpose of retrieving software and data; and
- has appropriate levels of physical security in place (i.e. software and data are stored in fire-rated safes and containers which are located behind access-controlled doors in areas accessible only by authorised personnel).

5.2 Procedural Controls

Administrative processes are dealt with and described in detail in the various documents used within and supporting the QuoVadis PKI.

Issuing CAs are required to ensure that administrative procedures related to personnel and procedural requirements, and physical and technological security mechanisms, are maintained in accordance with this CP/CPS and other relevant operational documents.

It is company policy that QuoVadis will not outsource any of its PKI operations to other organisations.

5.2.1 Trusted Roles

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

- Certification Authority Officers who are responsible for CA hardware and software and the generation and signing of Issuing CA Keys.
- Registration Authority Officers who are appointed by Registration Authorities, issued Registration Authority Certificates, and given responsibility for the operation of Registration Authority functions and the interface with the Issuing CA.
- QuoVadis Chief Security Officer who is responsible for verifying the integrity of the Certification Authorities and Registration Authorities and their operations and configurations.

5.2.2 Number of Persons Required Per Task

At least two people are assigned to each trusted role to ensure adequate support at all times, except for the role that performs the task of verifying and reviewing audit logs. Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure, most especially the Root Certification Authority and Issuing CA Private Keys, and customer Private Keys if held temporarily by QuoVadis during the registration process.

CA Key Pair generation and initialisation of a Root CA or Issuing CA shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

Issuing CAs will utilise commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. Issuing CAs must ensure that no single individual may gain access to any Private Key (other than the individual's own Private Key). At a minimum, procedural or operational mechanisms must be in place for Issuing CA key recovery in disaster recovery situations. To best ensure the integrity of the Issuing CA equipment and operation, Issuing CAs will use commercially reasonable efforts to identify a separate individual for each trusted role.

5.2.3 Identification and Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure, designated "Position of Trust".

Each individual performing any of the trusted roles shall use a QuoVadis issued Digital Certificate (i.e., a Utility Certificate) stored on a cryptographic smart card evaluated to at least Common Criteria EAL 4 to identify themselves to the Digital Certificate server and Repository.

5.2.4 Roles Requiring Separation of Duties

Operations involving Root Certificate and Issuing CA roles are segregated between M of N employees where M is equal to or greater than 2. (An M-of-N person control means there is a minimum "M" persons present out of a total "N" persons authorised to perform the task.) Creation and maintenance of system audit logs are segregated from those persons who operate such systems.

5.3 Personnel Controls

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

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

no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.1 Qualifications, Experience, and Clearance Requirements

QuoVadis requires that personnel meet a minimum standard with regards to Qualifications, Experience, Clearance and Training.

5.3.2 Background Check Procedures

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

- Previous employment
- Professional references
- Educational qualifications
- Criminal Records
- Credit/financial history and status
- Driving licenses
- Other relevant government records (e.g. national identifiers, etc.)

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

5.3.3 Training Requirements

QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities. This includes specific vetting training for Validation Specialists, who may not undertake Certificate validation and issuance until they have passed a suitable examination on knowledge and skills.

5.3.4 Retraining Frequency And Requirements

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

5.3.5 Job Rotation Frequency And Sequence

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

5.3.6 Sanctions for Unauthorised Actions

Appropriate disciplinary actions are taken for unauthorised actions.

5.3.7 Independent Contractor Requirements

QuoVadis does not support the use of independent contractors to fulfil trusted roles. Where appropriate, QuoVadis authorizes independent contractors to carry out identification and documentation activities for the issuance of non TLS/SSL certificates. These parties are contractually obliged to act in accordance with this CP/CPS including but not limited to training and data retention.

5.3.8 Documentation Supplied To Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types Of Events Recorded

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

QuoVadis logs the following events:

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

QuoVadis event logs include:

- Date and time of the entry
- Serial or sequence number of entry (for automatic journal entries)

- Details of the of entry (name, type etc)
- Source of entry (for example, terminal, port, location, customer, IP address)
- Destination address (if relevant)
- Identity of the entity making the journal entry (e.g. User ID)

5.4.2 Frequency Of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3 Retention Period For Audit Log

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

5.4.4 Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI.

Only certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction.

All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5 Audit Log Backup Procedures

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

Backup procedures apply to the QuoVadis PKI and the Participants therein including the QuoVadis Root Certification Authority, Issuing CAs and Registration Authorities.

5.4.6 Audit Collection System

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

5.4.7 Notification To Event-Causing Subject

Where an event is logged, no notice is required to be given to the Individual, Organisation, Device or Application that caused the event.

5.4.8 Vulnerability Assessment

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

5.5 Records Archival

5.5.1 Types Of Records Archived

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

- Audit logs;
- Digital Certificate requests and all related actions;
- Contents of issued Digital Certificates;
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Revocation requests and all related actions;
- Archive and retrieval requests;
- Digital Certificate Revocation Lists posted;
- Audit Opinions as discussed in this QuoVadis CP/CPS; and
- Name of the relevant QuoVadis Registration Authority.

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 Digital Certificates. Detailed system generated logs are retained for 18 months based on a risk assessment.

5.5.3 Protection Of Archive

Archives shall be retained and protected against modification or destruction. Only specific QuoVadis Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law.

QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.5.4 Archive Backup Procedures

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

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 system 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. QuoVadis provides assistance to Issuing CAs and Registration Authorities within the QuoVadis PKI to preserve their audit trails.

5.5.7 Procedures To Obtain And Verify Archive Information

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

5.6 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 and OCSP responder Certificates associated with that key. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

5.7 Compromise And Disaster Recovery

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

QuoVadis and each Issuing CA have in place an appropriate disaster recovery and business resumption plan that provides for the immediate continuation of Digital Certificate revocation services in the event of an unexpected emergency. QuoVadis regards its disaster recovery and business resumption plan as proprietary, security-sensitive, and confidential. Accordingly, it is not intended to be made generally available.

QuoVadis and each Issuing CA have in place an appropriate Key compromise plan detailing the activities taken in the event of a compromise of a QuoVadis Issuing CA Private Key. Such plans include procedures for:

- Revoking all Digital Certificates signed with that QuoVadis Issuing CA's Private Key; and
- Promptly notifying QuoVadis and all of the Holders of Digital Certificates issued by that QuoVadis Issuing CA.

5.7.1 QuoVadis Business Continuity Plan

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

- Incident and compromise handling procedures;
- Computing resources, software, and/or corrupted data handling procedures;
- Entity Private Key compromise procedures;
- Entity Public Key Revocation procedures; and
- Business continuity capabilities and procedures after a disaster.

5.8 Certification Authority And/Or Registration Authority Termination

When it is necessary to terminate an Issuing CA or Registration Authority service, the impact of the termination will be minimised as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements.

QuoVadis and each Issuing CA specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations. The procedures must, at a minimum:

- ensure that any disruption caused by the termination of an Issuing CA is minimised;
- ensure that archived records of the Issuing CA are retained;
- ensure that prompt notification of termination is provided to Certificate Holders, Authorised Relying Parties, and other relevant parties in the QuoVadis PKI;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained; and
- notify relevant Government and Certification bodies under applicable laws and related regulations.

For Qualified Certificates, in accordance with Swiss Digital Signature law, 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 European Qualified Certificates, in accordance with the eIDAS Regulation, 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.

5.8.1 User Keys And Certificates

Where practical, Key and Digital Certificate revocation should be timed to coincide with the progressive and planned rollout of new Keys and Digital Certificates by a successor Issuing CA.

5.8.2 Successor Issuing Certification Authority

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations and duties as the terminating Issuing CA. The successor Issuing CA should issue new Keys and Digital Certificates to all subordinate service providers and Users whose Keys and Digital Certificates were revoked by the terminating Issuing CA due to its termination, subject to the individual service provider or User making an application for a new Digital Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or Certificate Holder Agreement.

6 Technical Security Controls

The QuoVadis Certification Authority Private Keys are protected within a hardware security module meeting at least Federal Information Processing Standard-140-2 level 3 and/or EAL 4. Access to the modules within the QuoVadis environment, including the Root and Operational Digital Certification Authorities' Private Keys, are restricted by the use of token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the QuoVadis management team. Such 2-of-N allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

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

For Qualified Certificates of type QCP-n-qscd, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature Creation Device (QSCD).

For relevant European Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 and is certified to the appropriate standards..

In some cases, a Qualified Trust Service Provider (QTSP) generates and manages private keys on behalf of the Certificate Holder. This is signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in certificate policies. Refer to section 10.1.1 for further details.

6.1.2 Private Key Delivery To Certificate Holder

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

Where QuoVadis generates the private keys on behalf of the Certificate Holder, they are provided in a secure manner via the QuoVadis Trust/Link certificate management system.

For some EU Qualified Certificates, a Qualified Trust Service Provider (QTSP) generates and manages private keys on behalf of the Certificate Holder. Where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures shall only be created by the QSCD. In the case of natural persons, the Certificate Holders' 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.

6.1.3 Public Key Delivery To Certificate Issuer

Public Keys must be delivered in a secure and trustworthy manner, such as a Digital Certificate request message. Delivery may also be accomplished via non-electronic means. These means may include, but are not limited to, USB drive (or other storage medium) sent via registered mail or courier, or by delivery of a Token for local Key generation at the point of Digital Certificate issuance or request. Offline means will include Identity checking and will not inhibit establishing proof-of-possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a Certificate Holder Agreement or other agreement. In those cases where Key Pairs are generated by the Issuing CA on behalf of the Holder, the Issuing CA will implement secure mechanisms to ensure that the Token on which the Key Pair is held is securely sent to the proper Holder, and that the Token is not activated prior to receipt by the proper Holder.

6.1.4 Certification Authority Public Key To Relying Parties

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

6.1.5 Key Sizes

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

Currently QuoVadis generates and uses at least the following key sizes, signature algorithms and hash algorithms for signing Certificates, CRLs and certificate status server responses:

- 2048-bit RSA Key or 384-bit ECDSA key
- SHA-256 digest algorithm

6.1.6 Public Key Parameters Generation And Quality Checking

For Certificate Holders, the quality of parameters used to create Public Keys are determined by the relevant Registration Authority application or by the Certificate Holder's client application.

For QuoVadis, its Issuing CAs and Registration Authorities, all hardware and associated software platforms meet the requirements of FIPS 186-2, which ensures the proper parameters and their quality (e.g. random-generation and primality).

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

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

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

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

Keys may be used for the purposes and in the manner described in the QuoVadis CP/CPS – Digital Certificate Profiles.

An Issuing CA's Private Keys may be used for Digital Certificate signing and CRL and OCSP response signing. Keys may also be used to authenticate the Issuing CA to a Repository.

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 generation and maintenance of the Root and Issuing CA Private Keys are facilitated through the use of an advanced cryptographic device known as a Hardware Security Module. The Hardware Security Module used by Issuing CAs in the QuoVadis PKI are designed to provide at least Federal Information Processing Standard-140-2 Level 3 and/or EAL 4 security standards in both the generation and the maintenance in all Root and Issuing CA Private Keys.

For Qualified Certificates of type QCP-n-qscd, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature Creation Device (QSCD).

For relevant European Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.

In some cases, QuoVadis generates and manages private keys on behalf of the Certificate Holder 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. Refer to section 10.1.1 for further details.

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.

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

All CA Private Keys are accessed / activated through n-of-m multi-person control (e.g. a minimum threshold of splits of a Private Key decryption key must be used to decrypt or access the private CA signing key).

6.2.3 Private Key Escrow

Private Keys shall not be escrowed.

6.2.4 Private Key Backup

All Issuing CA Keys are held in secure cryptographic devices and are equally secured whenever stored outside the FIPS- boundary of the secure cryptographic device, never appearing in plaintext. Issuing CA Private Keys are stored in an encrypted state (using an encryption key to create a “cryptographic wrapper” around the key). Access is only by N- of-M control discussed above in Section 6.2.2. They are backed up under further encryption and maintained on-site and in secure off-site storage.

Certificate Holders may choose to backup their Private Keys by backing up their hard drive or the encrypted file containing their Keys.

6.2.5 Private Key Archive

The QuoVadis PKI does not support private key archive for TLS/SSL Certificates. Private Keys used for encryption shall not be archived, unless the Certificate Holder or Registration Authority specifically contracts for such services. Private Key archive is prohibited for QV Advanced+ and QV Qualified Certificates, or for any Private Key whose Key Usage is dedicated to Signing or Authentication.

Where a single Key Pair is generated for Signing and Encryption, the Private Key will only be archived on the specific request of the Certificate Holder and the corporate entity with which that Certificate Holder is affiliated.

Under no circumstances will Private Keys for Swiss or European Qualified Digital Certificates be archived.

6.2.6 Private Key Transfer Into Or From A Cryptographic Module

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

6.2.7 Private Key Storage On Cryptographic Module

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

6.2.8 Method Of Activating Private Key

A Certificate Holder must be authenticated to the Cryptographic Module before the activation of the Private Key. This Authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

6.2.9 Method Of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorised access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the Holder's sole control. Issuing CA Private Keys are not usually deactivated, but are kept in locked computer cabinets with appropriate physical and logical security controls. Other cryptographic modules used by QuoVadis are deactivated through a manual logout procedure or a passive timeout.

6.2.10 Method Of Destroying Private Key

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

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

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

6.2.11 Cryptographic Module Rating

The cryptographic modules used by the QuoVadis PKI are validated to FIPS 140-2 Level-3 and/or Common Criteria EAL 4 security standards.

For Qualified Certificates, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature Creation Device (QSCD)

For relevant Qualified Certificates, in accordance with the eIDAS Regulation, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature Creation Device (QSCD) meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards. Where QuoVadis manages the QSCD on behalf of the Certificate

Holder, QuoVadis operates the QSCD in accordance with Annex II of the eIDAS Regulation.

6.3 Other Aspects Of Key Pair Management

6.3.1 Public Key Archival

Public Keys will be recorded in Digital Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained.

6.3.2 Certificate Operational Periods And Key Pair Usage Periods

Usage periods for Public Keys and Private Keys shall match the usage periods for the Digital Certificate that binds the Public Key to an Individual, Organisation, or Device. Please see the variable Issuing Certificate Authority 'Valid From' and 'Valid To' fields in the Certificate Profiles outlined in Appendix A.

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

- Root CA Certificate 30 years
- All Issuing CA Certificates 10 – 15 years
- Qualified Certificates 1 to 3 years
  - Business SSL Certificates 825 days
  - EV SSL Certificates 2 years
- All other Digital Certificates Variable
  (But less than the remainder of the appropriate Issuing Certificate Authority Certificate)

6.4 Activation Data

6.4.1 Activation Data Generation And Installation

Two-factor authentication shall be used to protect access to a Private Key. One of these factors is a randomly and automatically generated key that protects the Private Key.

A unique Personal Identification Code may be generated by a Registration Authority during Key Pair creation, to protect the transport of the Keys and Digital Certificates to the Certificate Holder.

QuoVadis Certification Authority Officers are also required to use strong passwords to further prevent unauthorized access to CA systems.

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. Personal Identification Codes may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the Personal Identification Code. 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 Certificate Holder's personal information.

6.4.3 Other Aspects Of Activation Data

Where a Personal Identification Code is used, the User is required to enter the Personal Identification Code and identification details such as their distinguished name before they are able to access and install their Keys and Digital 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

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

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

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

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

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

QuoVadis has established an approved System Security Policy that incorporates computer security controls that are specific to QuoVadis and address the following:

6.6.1 System Development Controls

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

6.6.2 Security Management Controls

The QuoVadis Certificate Authority follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke and manage Public Key Certificates, such as X.509 Certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3 Life Cycle Security Controls

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

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

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

6.7 Network Security Controls

All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

Any and all unused network ports and services are turned off to ensure that Issuing CA equipment is protected against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone, off-line configurations.

6.8 Time-Stamping

The QuoVadis Time-stamping Authority uses PKI and trusted time sources to provide reliable standards-based time- stamps. The QuoVadis Time-stamp Policy defines the operational and management practices of the QuoVadis Time- stamp Authority such that Participants and Relying Parties may evaluate their confidence in the operation of the time- stamping services.

The QuoVadis Time-stamp Policy aims to deliver time-stamping services used in support of Qualified Electronic Signatures, as well as under applicable Swiss and Bermuda law and regulations. However, QuoVadis Time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The structure and content of the QuoVadis Time-stamp Policy is in accordance with ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time- Stamps. The QuoVadis Time-stamp Policy is administered and approved by the QuoVadis Policy Management Authority and should be read in conjunction with this CP/CPS.

7 Certificate, CRL, And OCSP Profiles For Certificates Which Do Not Include Server Authentication Key Use

7.1 Certificate Profile

All QuoVadis Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilise the ITU-T X.509 version 3 Digital Certificate standard.

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

7.1.1 Basic Certificate Contents

Fields	Content	Demarcation
Version	The version of the encoded certificate. QuoVadis certificates are Version 3	Fixed
Serial Number	Unique system generated random number assigned to each certificate, containing at least 64 bits of output.	Fixed
Signature Algorithm	The algorithm identifier for the algorithm used to sign the certificate.	Fixed
Issuer	Issuer is the entity that has signed and issued the certificate	
Common Name (CN)	Issuing Certification Authority Common Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Organisation legal name	Fixed
Country (C)	Issuing CA Jurisdiction	Fixed

Valid From	The date on which the Certificate validity period begins (MM/DD/YYYY HH:MM A.M/P.M)	Fixed
Valid To	The date on which the Certificate validity period ends MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject	The Subject field identifies the entity associated with the Public Key stored in the subject Public Key field	
Common Name (CN)	Subject Common Name	Holder Variable
Pseudonym (P)	Subject Pseudonym	Holder Variable
Title (T)	Subject Title (for example Dr.)	Holder Variable
Generation Qualifier	Subject Generation Qualifier (for example Jr.)	Holder Variable
Serial Number	Subject Serial Number	Holder Variable
Organisational Unit (OU)	Subject Organisational Unit	Holder Variable
Organisation (O)	Subject Organisation Name	Holder Variable
Locality (L)	Subject Locality	Holder Variable
State/Province (ST)	Subject State/Province	Holder Variable
Country (C)	Subject Country	Holder Variable
Subject email address	The e-mail address of the subject.	Holder Variable
Subject Public Key Information	Contains the Public Key and identifies the algorithm with which the Key is used	Fixed

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.

The table below describes common Certificate extensions that are included in QuoVadis Digital Certificates. Refer to Appendix A for Certificate extensions that are specific to the individual classes of Digital Certificates.

Fields	Content	Demarcation
Extensions		
Authority Key Identifier	Provides a means of identifying the Public Key corresponding to the Private Key used to sign a Certificate. This field contains the Subject Key Identifier of the issuer's Certificate.	Fixed
Subject Key Identifier	Provides a means of identifying Certificates that contain a particular Public Key. This field contains the ID of the Certificate Holder's key.	Fixed
Key Usage (Critical)	Defines the purpose of the key contained in the Certificate. Common Key Usages include: • digitalSignature • nonRepudiation • keyEncipherment Refer to section 10.1.2 for further information in relation to Key Usages.	
Certificate Policies	This extension contains Object Identifiers (OIDS) as well as a URL with a link to the QuoVadis Repository at https://www.quovadisglobal.com/repository. QuoVadis Certificates issued up to and including version 4.6 of this CP/CPS contain the OIDs for QuoVadis Root 1 (1.3.6.1.4.1.8024.0.1) or QuoVadis Root 3 (1.3.6.1.4.1.8024.0.3). QuoVadis Certificates issued from version 4.7 onwards will instead contain an OID that relates to the QuoVadis Certificate Class. Refer to section 10.1.1 for further information in relation to QuoVadis Certificate Classes and the related OIDS.	Fixed
Subject Alternative Name	This extension allows identities to be bound to the subject of the Certificate and can include Internet e- mail address, Microsoft UPN, a DNS name, IP address, or a Uniform Resource Identifier (URI). Refer to Appendix A for the Subject Alternative Name specific to each class of QuoVadis Certificates. All parts of the Subject Alternative Name included in the Digital Certificate will be subject to verification.	Holder Variable

Extended Key Usage (EKU)	This extension indicates one or more purposes for which the certified Public Key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. The main EKUs used by QuoVadis include: • smartcardlogon • clientAuth • emailProtection The EKU in QuoVadis Digital Certificates is dependent on the QuoVadis Certificate Class and the Key Usage. Refer to Appendix A.	Fixed
CRL Distribution Points	Identifies how CRL information is obtained. The following URL is included in QuoVadis Certificates: http://crl.quovadisglobal.com/<caname>.crl (where <caname> is the short name of the relevant CA)	Fixed
Authority Information Access	Indicates how to access information and services for the issuer of the Certificate. The following URLs are included in QuoVadis Certificates: • URL = http://ocsp.quovadisglobal.com • URL=http://trust.quovadisglobal.com/<caname>.crt (where <caname> is the short name of the relevant CA)	Fixed
Basic Constraints	Indicates whether the subject of the Digital Certificate is a CA and the maximum depth of valid certification paths that include this Certificate.	Fixed
Thumbprint Algorithm	The algorithm used to hash the Certificate	Fixed
Thumbprint	The system generated hash of the Certificate	Fixed

7.1.3 Algorithm Object Identifiers

No Stipulation.

7.1.4 Name Forms

See Appendix B.

7.1.5 Name Constraints

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

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

Effective 22nd June 2017, new Subordinate CA certificates issued to external entities who wish to operate their own subordinate CAs under a QuoVadis root include EKUs specifying all extended key usages that the subordinate CA is authorized to issue certificates for. The anyExtendedKeyUsage AND id-kp-serverAuth KeyPurposeIds MUST NOT appear within this extension. If the certificate includes the id-kp-emailProtection extended key usage, it MUST include the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees,each such name having its ownership validated.

7.1.6 CP/CPS Object Identifier

The Object Identifiers (OIDs) assigned to this CP/CPS are 1.3.6.1.4.1.8024.0.1 and 1.3.6.1.4.1.8024.0.3.

7.1.7 Usage Of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax And Semantics

Digital Certificates issued within the QuoVadis PKI contain one of the Object Identifiers for this CP/CPS and an Object Identifier representing the QuoVadis Certificate Class.

7.1.9 Processing Semantics For The Critical Certificate Policies Extension

No Stipulation.

7.2 Certificate Revocation List Profile

Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 5280.

7.2.1 Version Number

Issuing CAs within the QuoVadis PKI issue X.509 version 2 Certificate Revocation Lists.

7.2.2 Certificate Revocation List And Certificate Revocation List Entry Extensions

All User PKI software must correctly process all Certificate Revocation List extensions identified in the Digital Certificate and Certificate Revocation List profile.

7.3 Online Certificate Status Protocol Profile

Online Certificate Status Protocol is enabled for all Digital Certificates within the QuoVadis PKI.

7.3.1 Online Certificate Status Protocol Version Numbers

Version 1 of the Online Certificate Status Protocol, as defined by RFC2560, is supported within the QuoVadis PKI.

7.3.2 Online Certificate Status Protocol Extensions

No Stipulation.

7.4 Lightweight Directory Access Protocol Profile

QuoVadis will host a repository in the form of a Lightweight Directory Access Protocol directory for the purpose of (i) storing and making available all X.509 v. 3 Digital Certificates issued under the QuoVadis PKI, (ii) facilitating public access to download these Digital Certificates for Certificate Holder and relying party requirements, and (iii) receiving (from the QuoVadis PKI), storing and making publicly available, regularly updated Certificate Revocation List v. 2 information, for the purpose of Digital Certificate validation.

7.4.1 Lightweight Directory Access Protocol Version Numbers

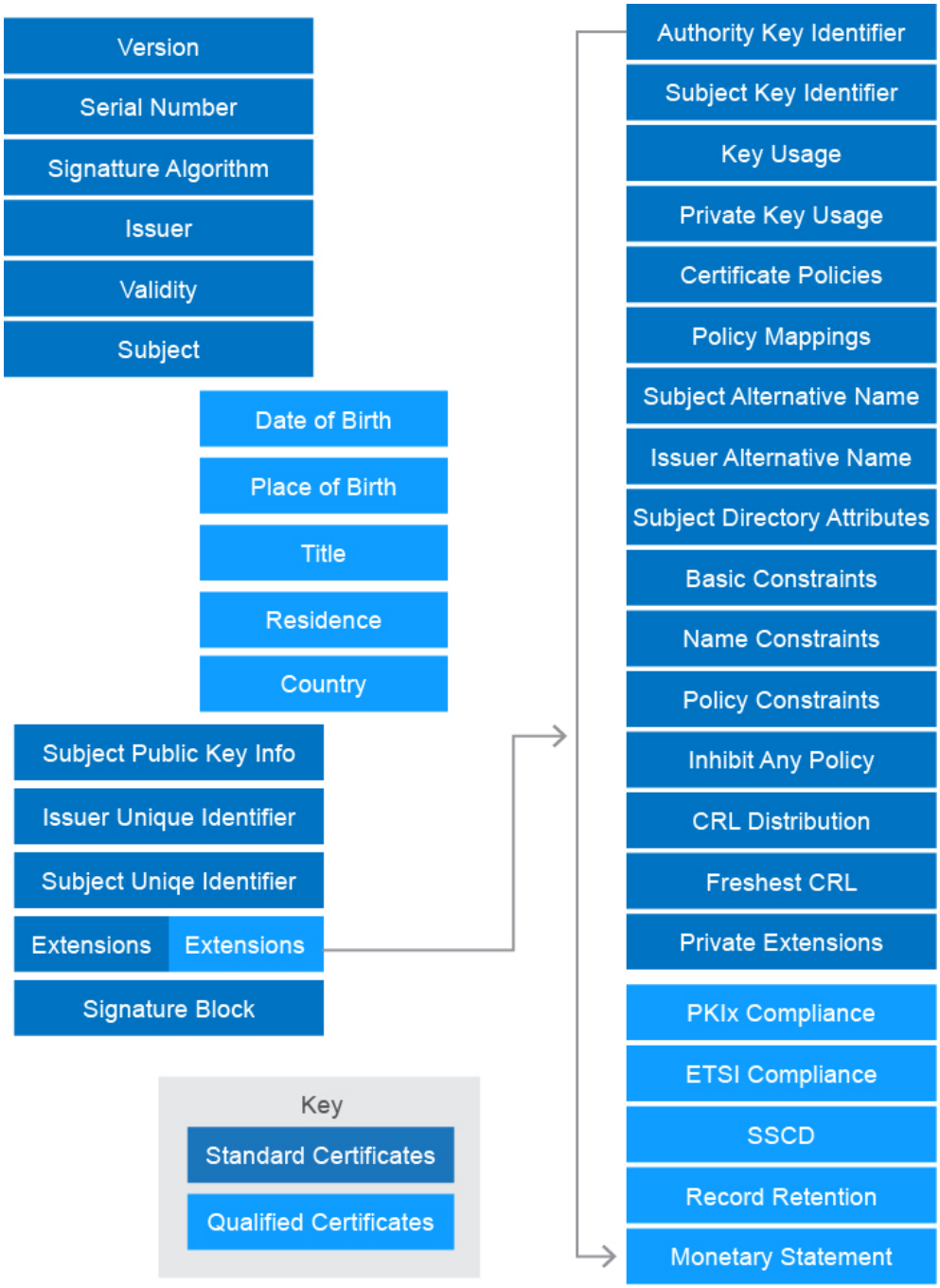
LDAP V3 in accordance with RFC-4510

7.4.2 Lightweight Directory Access Protocol Extensions

No Stipulation.

7.5 Digital Certificate Fields and Root CA Certificate Hashes

7.5.1 Digital Certificate Fields



7.5.2 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/QVRepository/DownloadRootsAndCRL.aspx.

7.5.2.1 QuoVadis Root CA Certificate Hashes

Field	Certificate Profile
Serial Number	3ab6508b
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash (sha1): 86 26 cb 1b c5 54 b3 9f bd 6b ed 63 7f b9 89 a9 80 f1 f4 8a Subject Key Id (precomputed): 8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Cert Hash(sha1): de 3f 40 bd 50 93 d3 9b 6c 60 f6 da bc 07 62 01 00 89 76 c9

7.5.2.2 QuoVadis Root CA 1 G3 Certificate Hashes

Field	Certificate Profile
Serial Number	78 58 5f 2e ad 2c 19 4b e3 37 07 35 34 13 28 b5 96 d4 65 93
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash (sha1): 92 ae ef 0e 89 02 ee 6d 79 68 d1 a1 0e 75 60 01 fa e4 eb fc Subject Key Id (precomputed): a3 97 d6 f3 5e a2 10 e1 ab 45 9f 3c 17 64 3c ee 01 70 9c cc Cert Hash(sha1): 1b 8e ea 57 96 29 1a c9 39 ea b8 0a 81 1a 73 73 c0 93 79 67

7.5.2.3 QuoVadis Root CA 3 Certificate Hashes

Field	Certificate Profile
Serial Number	05c6
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash(sha1): 14 8d b3 54 ed 9b 2f 13 08 7c c3 8b 4b c1 5b 96 8a c5 53 78 Subject Key Id (precomputed): f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Cert Hash(sha1): 1f 49 14 f7 d8 74 95 1d dd ae 02 c0 be fd 3a 2d 82 75 51 85

7.5.2.4 QuoVadis Root CA 3 G3 Certificate Hashes

Field	Certificate Profile
Serial Number	2e f5 9b 02 28 a7 db 7a ff d5 a3 a9 ee bd 03 a0 cf 12 6a 1d
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash (sha1): b7 1a 8b 40 df 93 d0 5c e0 98 03 08 91 59 6d 61 e8 15 f6 fe Subject Key Id (precomputed): c6 17 d0 bc a8 ea 02 43 f2 1b 06 99 5d 2b 90 20 b9 d7 9c e4 Cert Hash(sha1): 48 12 bd 92 3c a8 c4 39 06 e7 30 6d 27 96 e6 a4 cf 22 2e 7d

8 Compliance Audit and Other Assessments

8.1 Frequency, Circumstance And Standards Of Assessment

8.1.1 QuoVadis Certification Authority

QuoVadis CAs following this CP/CPS are subject to audits in respect of its various accreditations and certifications as follows:

Standards / Law	
Bermuda Accredited Certificate Service Provider	As defined in Bermuda's Electronic Transactions Act 1999, an Authorised Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.
WebTrust for Certification Authorities and WebTrust SSL Baseline	The WebTrust Seal of assurance for Certification Authorities (CA) symbolises to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria.
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 Inkrafttreten: 1.1.2017

ESI (“Directive”)	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
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 319 421	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 319 412-5	Certificate Profiles; Part 5: QCStatements
ETSI EN 319 422	Time stamping protocol and electronic time-stamp profiles
EUGridPMA	Accredited Certification Authority 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.

The results of these audits in the form of such publicly available audit reports as provided by the external auditors responsible for these audits will be published at

https://www.quovadisglobal.com/accreditations.aspx. Compliance audits as carried out under these provisions may substitute for audits noted in this CP/CPS.

8.1.2 Issuing Certification Authorities

Issuing CAs should be audited in accordance with the accreditations listed above. These audits shall include the review of all relevant documents maintained by the Issuing CA regarding operations within the QuoVadis PKI and under this QuoVadis CP/CPS, and other related operational policies and procedures.

8.1.3 Registration Authorities

Selected Registration Authorities within the QuoVadis PKI are subject to annual compliance reviews performed by or on behalf of QuoVadis in order to determine compliance by those entities with their operational requirements within the QuoVadis PKI. The obligations of Issuing CAs and Registration Authorities within the QuoVadis PKI is established by contract between those entities.

8.2 Identity And Qualifications Of Assessor

The audit services described in Section 8.1.1 are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and are experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies. The Bermuda Certificate Service Provider and WebTrust audits have been carried out by Ernst & Young. The accreditation audits for Swiss and European signature requirements have been performed by KPMG AG and BSI.

8.3 Assessor's Relationship To Assessed Entity

The auditor and the Issuing CA under audit, must not have any other relationship that would impair the auditor's 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

The topics covered by an audit of an Issuing CA will include but may not be limited to:

- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;

- Contracts; and
- Privacy Considerations.

8.5 Actions Taken As A Result Of Deficiency

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

For Qualified Certificates, in accordance with the Swiss Digital Signature law, the course of action and time frame for rectification of any deficiency as set by the accrediting authority Metas-SAS must be followed.

For Qualified Certificates, in accordance with the eIDAS Regulation, the course of action and time frame for rectification of any deficiency as set by the Conformity Assessment Body must be followed.

8.5.1 Issuing Certification Authorities

If irregularities are found, the Issuing CA in question must submit a report to the QuoVadis Root CA detailing actions the Issuing CA will take in response to the irregularity.

Where the Issuing CA fails to take appropriate action in response to an irregularity, the QuoVadis Root CA may (i) indicate the irregularities, but allow the Issuing CA to continue operations for a limited period of time; (ii) allow the Issuing CA to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation of that Issuing CA's Issuing Certificate; (iii) limit the class of any Digital Certificates issued by the Issuing CA; or (iv) revoke the Issuing CA's Issuing Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary cessation of the Issuing CA's services, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of any remedy.

In circumstances where any irregularities are found with respect to QuoVadis, in its capacity as an Issuing CA, the principles enunciated above will be followed by the QuoVadis Root CA.

8.5.2 Registration Authorities

If irregularities are found, the QuoVadis Root CA, or if applicable the Issuing CA, will address the issues raised with the relevant entity. Any action to be taken will be

determined by QuoVadis by reference to its determination as to the severity or materiality of the irregularity. In the event that QuoVadis determines that remedial action is required, the relevant entity will be advised by QuoVadis as to the procedures and action required to remedy the irregularity. Remedial action determined by QuoVadis shall be limited to the operations and procedures required to be taken in order to ensure that the Registration Authority operates in compliance with the QuoVadis CP/CPS. In the event that QuoVadis determines that remedial action is required, and such action is not taken in accordance with QuoVadis' determination, QuoVadis may (i) allow the Nominating Issuing CA to continue operations for a further period of time whilst the irregularities are addressed; (ii) allow the Nominating CA and its Registration Authority to continue operations for a maximum of thirty (30) days pending full implementation of the actions required by QuoVadis prior to termination of that Issuing CA's or Registration Authority's agreement with QuoVadis and the associated revocation of any Digital Certificate issued to them; (iii) limit the class of any Digital Certificates issued by the Nominating Issuing CA; or (iv) terminate that Issuing CA's agreement with QuoVadis and revoke the Issuing Certificate. Any decision regarding which of these actions to take will be based on QuoVadis' opinion of the severity and materiality of the irregularities.

8.6 Publication Of Audit Results

The audit opinion based on results of the audits will be generally available upon request. The results of the most recent audit of QuoVadis will be posted at https://www.quovadisglobal.com/accreditations.aspx.

8.7 Self Audits

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Issuing CAs and Registration Authorities within the QuoVadis PKI will make available all applicable fees upon request. Fees for Digital Certificate issuance vary widely based upon volumes and Digital Certificate types. Annual Fees for Qualified Certificate Holder Certificates issued to individual public applicants are €100.00 (Euro)

9.1.1 Certificate Issuance Or Renewal Fees

Fees may be payable with respect to the issuance or re-issuance of Digital Certificates - details of which are contained within the relevant contractual documentation governing the issuance or re-issuance of such Digital Certificates.

9.1.2 Certificate Access Fees

Fees may be payable with respect to access to the QuoVadis X.500 Directory services for Digital Certificate downloading, details of which are contained in relevant contractual agreements.

9.1.3 Revocation Or Status Information Access Fees

Fees may be payable with respect to access to the QuoVadis X.500 Directory services for Certificate revocation or status information, details of which are contained in relevant contractual agreements.

9.1.4 Fees For Other Services

Fees may be levied in connection with the following:

- Digital Certificate revocation;
- Private Encryption Key Archive and recovery;
- Digital Certificate status and Validation; and
- Policy access fees.

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

QuoVadis is responsible for maintaining its financial books and records in accordance with US GAAP and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

9.2.1 Insurance Coverage

QuoVadis maintains in full force and effect a liability insurance policy. In accordance with the requirement of ZERT ES, policy limits concerning Qualified Digital Certificates are maintained in excess of the minimum requirement of CHF 2 (Two) Million per occurrence and CHF 8 (Eight) Million annual aggregate.

Within the QuoVadis PKI the Root CA and all Issuing CAs and Registration Authorities are required to demonstrate that they have the financial resources necessary to discharge their obligations under this CP/CPS and any other relevant and associated documentation or agreements.

QuoVadis and each Issuing CA and/or Registration Authority shall maintain appropriate insurances necessary to provide for their respective liabilities as Participants within the QuoVadis PKI. Failure to establish and maintain insurances may be the basis for the revocation of their respective Digital Certificates.

9.2.2 Other Assets

Issuing CAs and Registration Authorities shall maintain sufficient assets and financial resources to perform their duties within the QuoVadis PKI and be reasonably able to bear liability to Certificate Holders and Relying Parties.

9.2.3 Insurance Or Warranty Coverage For End-Entities

QuoVadis will give advice to and support the QuoVadis Certificate Holders and QuoVadis Relying Parties on questions relating to the different types of insurance available.

QuoVadis Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the Private Key that corresponds to the Public Key in their QuoVadis Digital Certificate.

QuoVadis Relying parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.2.4 Fiduciary Relationships

QuoVadis is not the agent, fiduciary or other representative of any Certificate Holder and/or Relying Party and must not be represented by the Certificate Holder and/or Relying Party to be so. Certificate Holders 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 Certificate Holder 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 Digital 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

Any personal or corporate information held by Issuing CAs related to a Certificate Holder's application and the issuance of Digital 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 Certificate Holder or the Certificate Holder's Nominating Registration Authority, a copy of an entity's encryption Keys may be archived 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 Digital Certificates or stored in the Repository is not considered confidential, unless statutes or special agreements so dictate.

9.3.3 Responsibility To Protect Confidential Information

QuoVadis, Issuing CAs, Registration Authorities, Certificate Holders, Relying Parties and all others are responsible for protecting Confidential Business Information in their possession, custody or control.

9.4 Privacy Of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated As Private

All information about Certificate Holders that is not publicly available through the content of issued Digital Certificates, Digital Certificate directories or online Repositories is treated as private.

9.4.2.1 Registration Records

All registration records are considered confidential information and treated as private.

9.4.2.2 Certificate Revocation

Except for reason codes contained in a Certificate Revocation List, the detailed reason for a Digital Certificate being revoked, (if applicable), is considered to be confidential information, with the sole exception of the revocation of an Issuing CA's Issuing Certificate due to:

- the compromise of the Issuing CA's Private Key, in which case a disclosure may be made that the Private Key has been compromised; and
- the termination of an Issuing CA within the QuoVadis PKI, in which case prior disclosure of the termination may be given.

9.4.3 Information Deemed Not Private

9.4.3.1 Certificate Contents

The content of Digital Certificates issued by QuoVadis is public information and deemed not private.

9.4.3.2 Certificate Revocation List

Digital Certificates published in the X.500 Directory are not considered to be confidential information.

9.4.3.3 CP/CPS

This QuoVadis CP/CPS is a public document and is not confidential information and is not treated as Private.

9.4.4 Responsibility To Protect Private Information

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

9.4.5 Notice And Consent To Use Private Information

In the course of accepting a Digital Certificate, all Certificate Holders have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the QuoVadis Certification Authority, 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

9.4.6.1 Release To Law Enforcement Officials

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

With respect to the QuoVadis Root CA: or the laws of the jurisdiction of the relevant Issuing CA and enforceable in that jurisdiction.

9.4.6.2 Release As Part Of Civil Discovery

As a general principle, no document or record belonging to QuoVadis is released to any person except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to QuoVadis to be under appeal when served on QuoVadis (QuoVadis being under no obligation to determine the same), and which has been determined by a Court of competent jurisdiction to be valid, subsisting,

issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the relevant CA and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the CA (e.g. those of the relevant EU Member).

9.4.7 Other Information Disclosure Circumstances

QuoVadis, Issuing CAs and Registration Authorities are under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order that complies with requirements of this CP/CPS.

9.5 Intellectual Property Rights

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

Private Keys and Public Keys are the property of the applicable rightful Private Key holder. Digital Certificates issued and all Intellectual Property Rights including all copyright in all Digital Certificates and all QuoVadis documents (electronic or otherwise) belong to and will remain the property of QuoVadis.

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

9.5.1 Object Identifiers

QuoVadis is responsible for the Object Identifiers (OIDs) relating to the QuoVadis infrastructure. QuoVadis Object Identifiers start with 1.3.6.1.4.1.8024.

9.5.2 Licences

QuoVadis is in possession of, or holds licences for the use of, hardware and software in support of the QuoVadis PKI as outlined in this CP/CPS.

9.5.3 IETF Guidelines

The use of the PKIX IETF Guidelines is acknowledged.

9.5.4 Breach

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

9.6 Representations And Warranties

9.6.1 Certification Authority Representations

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

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

QuoVadis discharges its obligations by:

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

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

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

9.6.2 Registration Authority Representations and Warranties

9.6.2.1 Representations

Registration Authorities will perform their functions and will operate their certification services in accordance with:

- any Issuing CA Agreement;

- any applicable Registration Authority Agreement;
- all Certificate Policies under which they issue Digital Certificates;
- documented operational procedures; and
- applicable law and regulation.

9.6.2.2 Warranties

Authorised Registration Authorities operating within the QuoVadis PKI hereby warrant that (a) they take reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue, and (b) they will request that Digital Certificates be revoked by QuoVadis if they believe or are notified that the contents of the Digital Certificate are no longer accurate, or that the key associated with a Digital Certificate has been compromised in any way.

9.6.3 Certificate Holder Representations And Warranties

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

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

business and solely in accordance with the Certificate Holder Agreement; and

- Other Certificates: use the Certificate in accordance with all applicable laws, solely in accordance with the Certificate Holder Agreement and as may be reasonably used for its intended purpose.

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

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

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

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

9.6.4 Relying Parties Representations And Warranties

Relying Parties represent and warrant that:

- They will collect enough information about a Digital Certificate and its Corresponding Holder to make an informed decision as to the extent to which they can rely on the Digital Certificate.
- That they are solely responsible for making the decision to rely on a Digital Certificate.
- That they shall bear the legal consequences of any failure to perform Relying Party obligations under the terms of this CP/CPS and the Relying Party agreement.

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

To the extent permitted by applicable law, this CP/CPS, the Certificate Holder Agreement, the Relying Party Agreement, the Issuing CA Agreement, the Registration Authority Agreement and any other contractual documentation applicable within the QuoVadis PKI shall disclaim QuoVadis' possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, QuoVadis makes no express or implied representations or warranties pursuant to this CP/CPS. QuoVadis expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non infringement, merchantability, or fitness for a particular purpose.

9.8 Liability and Limitations of Liability

9.8.1 QuoVadis Liability

QuoVadis shall be liable to Certificate Holders or relying parties only for direct loss arising from any breach of this CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit specified below in section 9.8.3.1 for any one event or series of related events (in any one twelve-month period).

For Qualified Certificates, in accordance with the Swiss Digital Signature law, namely, Art 16 of Zert ES:

QuoVadis is liable to the Certificate Holder or the Relying Party who relies on a valid Qualified Certificate, for damages that arise because QuoVadis has not followed the procedures required by ZertES.

QuoVadis has the obligation to prove that such procedures were followed in accordance with ZertES.

QuoVadis cannot disclaim liability to either the Certificate Holder or Relying Party except where the Certificate Holder or Relying Party has not complied with the terms and conditions of use of the Certificate.

Sections 9.8.2; 9.8.3; 9.8.4; 9.8.5 DO NOT apply to Qualified Certificates.

For Qualified Certificates issued in accordance with eIDAS, QuoVadis is liable under the relevant sections of the eIDAS Regulation.

9.8.2 QuoVadis' Limitations Of Liability

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

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

9.8.3 Excluded Liability

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

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

9.8.3.1 Certificate Loss Limits

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

Loss Limits/ Reliance Limits	Maximum per Certificate
Advanced Certificates	US $250,000
Device Certificate	US $250,000
SuisseID Identity and Authentication (IAC) Certificates	CHF 10,000

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

9.8.4 Mitigation Of QuoVadis' Liability

QuoVadis has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by authorised personnel; or
- prohibit access to those resources by unauthorised individuals.

These measures include but are not limited to:

- identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
- performing regular system data backups;
- performing a backup of the current operating software and certain software configuration files;
- storing all backups in secure local and offsite storage;
- maintaining secure offsite storage of other material needed for disaster recovery;

- periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
- periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks; and
- periodically testing uninterrupted power supplies.

9.8.5 Claims Against QuoVadis Liability

9.8.5.1 Notification Period

QuoVadis shall have no obligation pursuant to any claim for breach of its obligations hereunder unless the claiming party gives notice to QuoVadis within ninety (90) days after the claiming party knew or ought reasonably to have known of a claim, and in no event more than three years after the expiration of the Digital Certificate held by the claiming party.

9.8.5.2 Mitigating Acts And Disclosure Of Supporting Information

As a precondition to QuoVadis' payment of any claim under the terms of this QuoVadis CP/CPS, a claiming party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such further agreements, instruments, and documents as QuoVadis may reasonably request in order to investigate a claim of loss made by a claiming party.

9.9 Indemnities

Notwithstanding any limitations on its liability to Certificate Holders and Relying Parties, QuoVadis acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with QuoVadis do not assume any obligation or potential liability of QuoVadis under this CP/CPs or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. QuoVadis shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by QuoVadis, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by QuoVadis where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from QuoVadis online, and the application software either failed to check such status or ignored an indication of revoked status).

Additional indemnity provisions and obligations are contained within relevant contractual documentation.

9.10 Term And Termination

9.10.1 Term

This CP/CPS becomes effective upon publication in the QuoVadis Repository. Amendments to this CP/CPS become effective upon publication in the QuoVadis Repository.

9.10.2 Termination

This CP/CPS shall remain in force until it is amended or replaced by a new version.

9.10.3 Effect Of Termination And Survival

The provisions of this QuoVadis CP/CPS shall survive the termination or withdrawal of a Certificate Holder or Relying Party from the QuoVadis PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the QuoVadis PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11 Individual Notices And Communications With Participants

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

9.12 Amendments

9.12.1 Procedure For Amendment

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

There are two possible types of policy change:

- the issue of a new CP/CPS; or
- a change to or alteration of a policy stated in an existing CP/CPS.

If an existing CP/CPS requires re-issue, the change process employed is the same as for initial publication, as described above. If a policy change is determined to have a material impact on a significant number of Certificate Holders and relying parties, then QuoVadis may, at its sole discretion, assign a new object identifier for Digital Certificates issued pursuant to the modified CP/CPS.

The only changes that may be made to this CP/CPS without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the QuoVadis PMA, materially impact any Participants within the QuoVadis PKI.

Issuing CAs are notified of changes to the CP/CPS as and when they are approved.

9.12.2 Notification Mechanism And Period

New or amended CP/CPSs are published on the web site at https://www.quovadisglobal.com/repository.

Any change that increases the level of trust* that can be placed in Digital Certificates issued under this CP/CPS or under policies that make reference to this CP/CPS requires thirty (30) days prior notice. Any change that decreases the level of trust that can be placed in Digital Certificates issued under this CP/CPS or under policies that make reference to this CP/CPS requires forty-five (45) days prior notice. The QuoVadis CP/CPS applicable to any Digital Certificate supported by this CP/CPS shall be the QuoVadis CP/CPS currently in effect.

* NOTE: In this section, "level of trust" does not include those parts of the specification relating to the liabilities of the parties. Reference to "level of trust" applies solely to the technical/administrative functions and any changes provided for under this clause shall not materially change this specification unless there is a significant business reason to do so.

9.12.3 Circumstances Under Which Object Identifiers Must Be Changed

The QuoVadis Policy Management Authority reserves the right to amend this CP/CPS without notification for amendments that are not material, including corrections of typographical errors, changes to URLs and changes to contact details. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the QuoVadis Policy Management Authority. Unless the QuoVadis Policy Management Authority determines otherwise, the Object Identifier to this CP/CPS shall not change.

9.13 Dispute Resolution Provisions

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

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

For Swiss Qualified Certificates, in accordance with the Swiss Digital Signature law, 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 Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

- Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.
- Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.
- Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

For Qualified Certificates, in accordance with the Swiss Digital Signature law, all disputes shall be dealt with under Swiss Law.

For Qualified Certificates, in accordance with the Dutch Digital Signature law, all disputes shall be dealt with under Dutch Law. For Qualified Certificates issued in other jurisdictions, disputes will be dealt with under the national law of the relevant Member State.

For Qualified Certificates, in accordance with the Belgian Digital Signature law, all disputes shall be dealt with under Belgian Law. For Qualified Certificates issued in other jurisdictions, disputes will be dealt with under the national law of the relevant Member State.

9.15 Compliance With Applicable Law

This CP/CPS is subject to applicable law.

9.16 Miscellaneous Provisions

Not Applicable.

9.16.1 Entire Agreement

Not Applicable.

9.16.2 Assignment

Not Applicable.

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees And Waiver Of Rights)

The failure or delay of QuoVadis to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by this QuoVadis CP/CPS shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of this QuoVadis CP/CPS is intended to be exclusive of any other right or remedy, except as expressly provided in this QuoVadis CP/CPS, and each and every right or remedy

shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

9.16.5 Force Majeure

QuoVadis accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters. See also Section 9.8.3 (Excluded Liability) above.

9.17 Other Provisions

No Stipulation.

10 APPENDIX A

10.1 Digital Certificate Profiles

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

Procedures for Certificate Holder registration as well as descriptions of fields are described below for each type of Digital 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

QuoVadis Certificate Class	Description	QuoVadis / ETSI Certificate 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 ETSI policy identifier OID: 0.4.0.2042.1.3	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 ETSI policy identifier OID: 0.4.0.2042.1.1	Medium	Optional
QV Advanced +	Similar to the "QV Advanced" _Certificate Class issued on a Secure Cryptographic Device. Based on the ETSI Normalised Certificate Policy requiring a secure cryptographic device (NCP+), which has the OID 0.4.0.2042.1.2	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300 ETSI policy identifier OID: 0.4.0.2042.1.2	High	Yes Adobe AATL Approved

QV Qualified	QuoVadis Qualified Certificate on a Qualified Signature Creation Device (QSCD), where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.400 ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)	High	Yes Adobe AATL Approved
	QuoVadis Qualified Certificate on a Qualified Signature Creation Device (QSCD), where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.410	High	Yes
	Relevant to the Policy in ETSI EN 319 411-2 for: EU qualified certificates issued to a natural person (QCP-n-qscd), with the policy identifier OID 0.4.0.194112.1.2 EU qualified certificates issued to a legal person (QCP-l-qscd), with the policy identifier OID 0.4.0.194112.1.3	ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)		
	QuoVadis Qualified Certificate not on a Qualified Signature Creation Device (QSCD). Relevant to the Policy in ETSI EN 319 411-2 for: EU qualified certificates issued to a natural person (QCP-n), with the policy identifier OID 0.4.0.194112.1.0 EU qualified certificates issued to a legal person (QCP-l), with the policy identifier OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 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 TLS/SSL Certificates. Includes Domain Controller certificates and Gateway certificates.	1.3.6.1.4.1.8024.1.600	Medium	Optional

10.1.2 Key Usage and Archive

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

QuoVadis Certificate Type	Key Usage/ Extended Key Usage	Applicability of Certificate Types to QuoVadis Certificate Classes			
		QV Standard	QV Advanced	QV Advanced +	QV Qualified
Signing and Encryption	**Key Usage** digitalSignature nonRepudiation keyEncipherment **Extended Key Usage** smartcardlogon clientAuth emailProtection	Allowed (Archival only permitted for certain Issuing CAs. Not permitted for any CAs on EU Trust Service Lists)	Allowed (Archival only permitted for certain Issuing CAs. Not permitted for any CAs on EU Trust Service Lists)	Allowed (Archival not permitted)	Not Allowed
Signing	**Key Usage** digitalSignature nonrepudiation **Extended Key Usage** smartcardlogon clientAuth emailProtection	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)
Encryption	**Key Usage** keyEncipherment **Extended Key Usage** emailProtection	Allowed (Archival permitted)	Allowed (Archival permitted)	Allowed (Archival not permitted)	Not Allowed
Authentication	**Key Usage** digitalSignature **Extended Key Usage** smartcardlogon clientAuth	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Not Allowed

The Certificate Profiles that follow indicate the fields which are VARIABLE on initial registration by the Certificate Holder (“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 Digital 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 Digital 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 Certificate Holder.

Fields	Content		Demarcation
Subject			
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com		Holder Variable
Common Name (CN)	Common Name		Holder Variable
givenName (natural person certs)	givenName (natural person certs)	Can use Pseudonym instead of givenName and surname	Holder Variable
Surname (natural person certs)	Surname (natural person certs)		Holder Variable
Organisational Unit (OU)	Variable Data		Holder Variable
Organisation (O)	Organisation legal name		Natural Person Certs: Optional Legal Person
OrganisationIdentifier	Holds an identification of an organisation different from the organisation name.		
Country/Locality	Variable Data		Holder Variable
Subject Public Key Information	RSA (2048-bit2048-bit) / System Generated		Fixed
Extensions			
Subject Alternative Name	Principle Name = Email Address		Holder Variable
Certificate Policies	This extension includes the QV Standard Certificate Class OID = 1.3.6.1.4.1.8024.1.100.		Fixed
	Certain certificates include the ETSI LCP OID = 0.4.0.2042.1.3		Fixed

10.3 QV Advanced

Purpose

QV Advanced Digital Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, encryption, and authentication.

Registration Process

Validation procedures for QuoVadis Advanced Digital Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1.

Unless the Certificate Holder has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Certificate Holder shall include the following:

If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

If the subject is a natural person evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

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

- Full name and legal status of the associated legal person;
- Any relevant existing registration information (e.g. company registration) of the associated legal person; and
- Evidence that the Certificate Holder is affiliated with the legal person.

If the Certificate Holder is a legal person (organisational entity), evidence shall be provided of:

- Full name of the legal person; and
- Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name.

If the Certificate Holder is a device or system operated by or on behalf of a legal person, evidence shall be provided of:

- identifier of the device by which it may be referenced (e.g. Internet domain name);
- full name of the organisational entity;
- a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

Fields	Content		Demarcation
Subject			
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com		Holder Variable
Common Name (CN)	Common Name		Holder Variable
givenName (G)	Given Name	Used for natural person certificates. Can use Pseudonym instead of givenName and surname	Holder Variable
Surname (S)	Surname		Holder Variable
Organisational Unit (OU)	Variable Data		Holder Variable
Organisation (O)	Organisation legal name		Natural Person Certs: Optional Legal Person Certs: Required
OrganisationIdentifier	Holds an identification of an organisation different from the organisation name.		
Country/Locality	Variable Data		Holder Variable
Subject Public Key Information	RSA (2048-bit2048-bit) / System Generated		Fixed
Extensions			
Subject Alternative Name	Principle Name = Email Address		Holder Variable
Certificate Policies	This extension includes the QV Advanced Certificate Class OID = 1.3.6.1.4.1.8024.1.200.		Fixed
	Certain certificates include the ETSI NCP OID = 0.4.0.2042.1.1		Fixed

10.4 QV Advanced +

Purpose

QuoVadis Advanced+ Digital Certificates are used for the same purposes as QuoVadis Advanced Digital 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).

Swiss Regulated Certificates issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ certificate class. These certificates are issued out of the “QuoVadis Swiss Regulated CA G1” and have the notice text “regulated certificate” in the CertificatePolicies user notice. Swiss Regulated Certificates can be issued to natural and legal persons.

Registration Process

QuoVadis Advanced+ Digital Certificates are based on with the Normalised Certificate Policy (NCP+) described in ETSI EN 319 411-1.

Unless the Certificate Holder has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Certificate Holder shall include the following:

If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

If the subject is a natural person evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

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

- Full name and legal status of the associated legal person;
- Any relevant existing registration information (e.g. company registration) of the associated legal person; and
- Evidence that the Certificate Holder is affiliated with the legal person.

If the Certificate Holder is a legal person (organisational entity), evidence shall be provided of:

Full name of the legal person; and

Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name.

If the Certificate Holder is a device or system operated by or on behalf of a legal person, evidence shall be provided of:

- identifier of the device by which it may be referenced (e.g. Internet domain name);
- full name of the organisationorganisational entity;
- a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organisationorganisational entity from others with the same name.

QuoVadis Advanced+ Digital Certificates must be issued on a Secure Cryptographic Device and adhere to the following requirements:

- Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA or RA;
- User activation data is securely prepared and distributed separately from the Secure Cryptographic Device;

Fields	Content		Demarcation
Subject			
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com		Holder Variable
Common Name (CN)	First Name - Last Name		Holder Variable
givenName (G)	Given Name	Used for natural person certificates. Can use Pseudonym instead of givenName and surname	Holder Variable
Surname (S)	Surname		Holder Variable
Organisational Unit (OU)	Variable Data		Holder Variable
Organisation (O)	Organisation legal name		Holder Variable
OrganisationIdentifier	Holds an identification of an organisation different from the organisation name.		Holder Variable
Country/Locality	Variable Data		Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated		Fixed
Extensions			
Subject Alternative Name	Principle Name = Email Address		Holder Variable
Certificate Policies	This extension includes the QV Advanced + Certificate Class OID = 1.3.6.1.4.1.8024.1.300.		Fixed
	Certain certificates include the ETSI NCP+ OID = 0.4.0.2042.1.2		Fixed
	Notice Text= regulated certificate		Only for Swiss Regulated Certificates

Adobe OIDs	Note these Adobe OIDs are only relevant for signing Certificates.	
Adobe Time Stamp (OID = 1.2.840.113583.1.1.9.1)	http://tsa01.quovadisglobal.com/TSS/HttpTspServer	Fixed
Adobe Archive RevInfo (OID = 1.2.840.113583.1.1.9.2)	This relates to OCSP revocation checking within Adobe products for long term validation purposes.	Fixed

10.4.1 EIDI-V/GeBüV Certificates

The procedure below assumes an application by a company or organisation on behalf of its employees or devices for Digital Certificates.

Purpose
The EIDI-V/GeBüV Certificate is issued to organisations (companies, municipalities, etc.) and issued primarily to digitally sign electronic invoices. The Certificates may also be used for commercial purposes (such as legally-compliant electronic archiving according to GeBüV).

Registration Process
These Digital Certificates are issued in accordance with EIDI-V (SR 641.201.1 and SR 641.201.1.1). Validation of these Certificates is performed in accordance with the validation procedures for QuoVadis Qualified Certificates and any additional validation requirements required by EIDI-V.

Fields	Content	Demarcation
Subject		
Common Name (CN)	Commercial Subject Name or First Name - Last Name	Holder Variable
Organisational Unit (OU)	Variable Data	Holder Variable
Organisational Unit (OU)	Accounting Services (OeIDI)/Third Party Services (art. 9 OeIDI)	Fixed
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Variable Data	Holder Variable
State/Province (ST)	Variable Data	Holder Variable
Country (C)	Variable Data	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage	Digital Signature	Fixed

Key Usage	Non Repudiation	
Certificate Policies	OID = 1.3.6.1.4.1.8024.0.1.0.0.1 (This is the QuoVadis EIDI-V OID)	Fixed
Policy Qualifier User Notice	Gestuetzt auf Art. 2 Abs. 2 EIDI-V; en vertu de l'art 2 al. 2 OeIDI; visto l'art. 2 cpv. 2 OeIDI; based on art. 2 para. 2 OeIDI; SR 641.201.511 / RS 641.201.511 Schweiz/Suisse/Svizzera/Switzerland	Fixed
Certificate Policies	1.3.6.1.4.1.8024.1.300 (This is the QV Advanced + Certificate Class OID)	Fixed
Policy Qualifier CPS	https://www.quovadisglobal.com/repository	
Subject Alternative Name	Commercial register identification number (ASN-1 printableString coded)	Holder Variable
Subject Alternative Name	Email Address (RFC 822 Name)	Holder Variable
Issuer Alternative Name	O=ZertES Recognition Body: KPMG AG	Fixed
Adobe Time Stamp (OID = 1.2.840.113583.1.1.9.1)	http://tsa01.quovadisglobal.com/TSS/HttpTspServer	Fixed
Adobe Archive RevInfo (OID = 1.2.840.113583.1.1.9.2)	This relates to OCSP revocation checking within Adobe products for long term validation purposes.	Fixed

10.4.2 SuisseID Identity and Authentication Certificates

Purpose

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Identity and Authentication (IAC) Certificates help provide strong and secure authentication to applications.

Either a Common Name or a Pseudonym is required for a QuoVadis SuisseID IAC Certificate. Use of both Common Name and Pseudonym in the same Certificate is not permitted.

Registration Process

QuoVadis SuisseID IAC Certificates are issued in accordance with the SuisseID requirements (including the "SuisseID Specification" document) using the QuoVadis SuisseID Signing Service. Unless stated otherwise in the SuisseID Specification document, the guidelines in TAV-ZERTES apply to the specification of QuoVadis SuisseID IAC Certificates.

For the issuance and life cycle management of SuisseID IAC Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant qualified certificate.

Evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical

presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognized 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 Certificate Holder is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorization from an authorized Organisation representative; and
- Evidence that the Certificate Holder is associated with the organisational entity.

Private Keys for SuisseID IAC Certificates are generated and stored on a Hardware Security Module that meets FIPS PUB 140-2, level 3 or EAL 4 standards. This Hardware Security Module is located in a QuoVadis data centre. Access by the Certificate Holder 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 QSCD.

QuoVadis SuisseID IAC Certificates have a maximum validity of three years.

Fields	Content	Demarcation
Signature Algorithm	sha256RSA	
Subject		
Common Name (CN)	First Name - Last Name (Authentication)	Holder Variable
Pseudonym	Pseudonym (Authentication)	Holder Variable
Title	Title (e.g. Dr.) which must be as written in ID Document/ Passport)	Holder Variable
Serial Number	1200-xxxx-xxxx-xxxx	Fixed
Organisational Unit (OU)	Variable Data	Holder Variable
Organisation (O)	Organisation legal name	Holder Variable
Locality	Locality	Holder Variable
State/Province	State/Province	Holder Variable
Country	Country	Holder Variable
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed

Extensions		
Key Usage (Critical)	DigitalSignature	Fixed
Certificate Policies		
CertPolicyID (SuisseID)	2.16.756.5.26.1.1.2	Fixed
User Notice	SuisseID identity and authentication certificate	Fixed
CertPolicyID (QuoVadis Certificate Class)	1.3.6.1.4.1.8024.1.300	Fixed
URL	https://www.quovadisglobal.com/repository	Fixed
Subject Alternative Name		
RFC822 email address	RFC822 email address (same as subject email address)	Holder Variable
Microsoft UPN	MUST be in the format: <SuisseID Number>@upn.suisseid.ch	Holder Variable
Extended Key Usage	Client Authentication	Fixed
Extended Key Usage	Secure Email	Fixed
Extended Key Usage	Smart Card Logon (Required if MS UPN in Subject Alternative Name field)	Fixed

10.5 QV Qualified - eIDAS

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 Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS Regulation”).

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key.

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).

Swiss Qualified certificates issued under the Swiss Federal signature law (ZertES) also meet this ETSI policy QCP-n- qscd. These Swiss Qualified certificates are issued only to natural persons out of the “QuoVadis Swiss Regulated CA G1” and have the notice text “qualified certificate” in the CertificatePolicies user notice.

The content of these certificates meet the relevant requirements of:

- 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 319 412-5: Certificate Profiles; Part 5: QCStatements

Registration Process

Identity validation procedures for these Digital 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.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

by the physical presence of the natural person; or

using methods which provide equivalent assurance in terms of reliability to the physical presence and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

Evidence may be provided on behalf of the subject by the RA. However, the subject remains responsible for the content of the certificate.

If the Certificate Holder is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Certificate Holder is associated with the organisational entity.

These Digital Certificates require a Qualified Signature Creation Device (QSCD) that meets the requirements laid down in annex II of Regulation (EU) N° 910/2014.

Fields	Content		Demarcation
Subject			
CommonName (CN)	CommonName		Required
givenName (G)	Given Name	Can use Pseudonym instead of givenName and surname	Required
Surname (S)	Surname		
SerialNumber (SN)	If serialNumber is present then it must be in the following structure as per section 5.1.3 of ETSI EN 319 412-1: • 3 character natural identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).		Optional
Organisation (O)	Organisation Legal Name		Optional
OrganisationIdentifier	Holds an identification of an organisation different from the organisation name.		Optional
Organisation Unit (OU)	Organisation Unit Name		Optional
Locality	Locality		Optional
State / Province (ST)	State or Province		Optional
Country (C)	Country		Required
email	Subject email		Optional
Subject Public Key Info	RSA (2046 Bits)		Fixed
Extensions			Fixed
KeyUsage (CRITICAL)	Non Repudiation		Fixed

Certificate Policies	1.3.6.1.4.1.8024.1.400 or 1.3.6.1.4.1.8024.1.410 (Cert Class: QV Qualified QSCD)	Fixed
	https://www.quovadisglobal.com/repository	Fixed
	0.4.0.194112.1.2 (QCP-n-qscd)	Fixed
	Notice Text= qualified certificate	Only for Swiss Qualified Certificates
Subject Alternative Name	Email Address (RFC 822 Name)	Optional
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 Certificate Holder with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.

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:

- 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 319 412-5: Certificate Profiles; Part 5: QCStatements

Registration Process

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 forthe “Policy for EU qualified certificate issued to a natural person” (QCP-n). QuoVadis recommends that QCP-n certificates are used only for electronic signatures.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

I. by the physical presence of the natural person; or

II. using methods which provide equivalent assurance in terms of reliability to the physical presence and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 Certificate Holder is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Certificate Holder is associated with the organisational entity.

Fields	Contents		Demarcation
Subject			
CommonName (CN)	CommonName		Required
givenName (G)	Given Name	Can use Pseudonym instead of givenName and surname	Required
Surname (S)	Surname		
SerialNumber (SN)	If serialNumber is present then it must be in the following structure as per section 5.1.3 of ETSI EN 319 412-1: • 3 character natural identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).		Optional
Organisation (O)	Organisation Legal Name		Optional

OrganisationIdentifier	Holds an identification of an organisation different from the organisation name.	Optional
Organisation Unit (OU)	Organisation Unit Name	Optional
Locality	Locality	Optional
State / Province (ST)	State or Province	Optional
Country (C)	Country	Required
email	Subject email	Optional
Subject Public Key Info	RSA (2046 Bits)	Fixed
Extensions		Fixed
KeyUsage (CRITICAL)	Non Repudiation	Fixed
Certificate Policies	1.3.6.1.4.1.8024.1.450 (Cert Class: QV Qualified - no QSCD)	Fixed
	https://www.quovadisglobal.com/repository	Fixed
	0.4.0.194112.1.0 (QCP-n)	Fixed
Subject Alternative Name	Email Address (RFC 822 Name)	Optional
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 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

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 Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person certificates an updated version of this CP/CPS will be published.

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key.

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.

The content of these certificates meet the relevant requirements of:

- 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

Registration Process

Identity validation procedures for these Digital 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).

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

I. by the physical presence by an authorized representative of the legal person; or

II. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name of the organisational entity (private organisation, government entity, business entity or non- commercial entity) consistent with the national or other applicable identification practices); and
- When applicable, the association between the legal person and the 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.

For the authorized representative of the legal person, evidence shall be provided of:

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

- Date and place of birth, reference to a 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.

These Digital Certificates require a Qualified Signature Creation Device (QSCD) that meets the requirements laid down in annex II of Regulation (EU) N° 910/2014.

Fields	Contents	Demarcation
Subject		
CommonName (CN)	CommonName	Required
Organisation (O)	Full registered name of the subject (legal person)	Required
OrganisationIdentifier	Since the semantics identifier is present in qcStatement this field must be in the following format as per section 5.1.4 of ETSI EN 319 412-1: • 3 character legal person identity type reference (e.g. NTR or VAT); • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference). Company registration number	Required
Organisation Unit (OU)	Organisation Unit Name	Optional
Locality	Locality	Optional
State / Province (ST)	State or Province	Optional
Country (C)	Country	Required
email	Subject email	Optional
Subject Public Key Info	RSA (2046 Bits)	Fixed
Extensions		Fixed
KeyUsage (CRITICAL)	Non Repudiation	Fixed
Certificate Policies	1.3.6.1.4.1.8024.1.400 or 1.3.6.1.4.1.8024.1.410 (Cert Class: QV Qualified QSCD)	Fixed
	https://www.quovadisglobal.com/repository	Fixed
	0.4.0.194112.1.3 (QCP-l-qscd)	Fixed
Extended KeyUsage	Document Signing (1.3.6.1.4.1.311.10.3.12)	Fixed
	E-mail protection (1.3.6.1.5.5.7.3.4)	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 2 = Certificate for electronic Seals 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)	0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is included in QuoVadis Certificates	Fixed

10.5.4 eIDAS Qualified Certificate issued to a legal person

Purpose

The purpose of these EU Qualified certificates are to identify the Certificate Holder with a high level of assurance, for the purpose of creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person certificates an updated version of this CP/CPS will be published.

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:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- loggETSI 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

Registration Process

Identity validation procedures for these Digital 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:

I. by the physical presence by an authorized representative of the legal person; or

II. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name of the organisational entity (private organisation, government entity, business entity or non- commercial entity) consistent with the national or other applicable identification practices); and
- When applicable, the association between the legal person and the 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.

For the authorized representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.

Fields	Contents	Demarcation
Subject		
CommonName (CN)	CommonName	Required
Organisation (O)	Full registered name of the subject (legal person)	Required
OrganisationIdentifier	Since the semantics identifier is present in qcStatement this field must be in the following format as per section 5.1.4 of ETSI EN 319 412-1: • 3 character legal person identity type reference (e.g. NTR or VAT); • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference). Company registration number	Required
Organisation Unit (OU)	Organisation Unit Name	Optional
Locality	Locality	Optional
State / Province (ST)	State or Province	Optional
Country (C)	Country	Required
Subject Public Key Info	RSA (2046 Bits)	Fixed
Extensions		Fixed
KeyUsage (CRITICAL)	Non Repudiation	Fixed
Certificate Policies	1.3.6.1.4.1.8024.1.450 (Cert Class: QV Qualified - no QSCD)	Fixed
	https://www.quovadisglobal.com/repository	Fixed
	0.4.0.194112.1.1 (QCP-l)	Fixed
Extended KeyUsage	Document Signing (1.3.6.1.4.1.311.10.3.12)	Fixed
	E-mail protection (1.3.6.1.5.5.7.3.4)	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-QcType (0.4.0.1862.1.6) id-etsi-qcs-6	esi4-qcStatement-6: Type of certificate 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) 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)	0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is included in QuoVadis Certificates	Fixed

10.6 QV Qualified - Legacy

10.6.1 Qualified Certificate Profile

Qualified certificates issued for natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under the eIDAS Regulation until they expire.

Purpose

The purpose of a Qualified Digital Certificate is to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified electronic signatures meeting the qualification requirements defined by the applicable legal framework of the Electronic Signatures Directive (1999/93/EC).

Registration Process

Validation procedures for QuoVadis Qualified Digital Certificates are consistent with the relevant requirements of ZertES, ETSI and eIDAS.

If the Certificate Holder is a physical person, evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 Certificate Holder is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Certificate Holder is associated with the organisational entity.

QuoVadis Qualified Digital Certificates require a Secure Signature Creation Device (SSCD) that meets the following requirements:

- SSCD storage, preparation, and distribution is securely controlled by CA or RA;
- User activation data is securely prepared and distributed separately from the SSCD;
- If keys are generated under the Certificate Holder's control, they are generated within the SSCD used for signing or decrypting;
- The Certificate Holder's Private Key can be maintained under the subject's sole control; and
- Only use the Certificate Holder's Private Key for signing or decrypting with the SSCD.

Fields	Contents	Demarcation
Signature Algorithm	sha256RSA	
Subject		
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	Holder Variable
Common Name (CN)	Common Name	Holder Variable
Surname (SN)	Surname (Optional)	Holder Variable
Given Name (G)	Given Name (Optional)	Holder Variable
Organisational Unit (OU)	Organisational Unit	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Not Stipulated	Holder Variable
State or Province	Not Stipulated	Holder Variable
Country	ISO Country Code	Holder Variable
Date Of Birth	DD/MM/YYYY	Holder Variable
Place of Birth	City	Holder Variable
Gender	M/F	Holder Variable
Title	Verified Legal Title	Holder Variable
Country of Residence	ISO Country Code – Normally Resident	Holder Variable
Country of Citizenship	ISO Country Code – Nationality	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		Fixed
Key Usage	Digital Signature Non Repudiation	Holder Variable Fixed
Subject Alternative Name	Principal Name = Email Address	Holder Variable
QC Statement PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed
QC Statement ETSI Compliance	0.4.0.1862.1.1	Fixed
Monetary Statement	Optional field. A monetary limit on the value of transactions for which the Certificate can be used. (OID 0.4.0.1862.1.2)	Holder Variable
SSCD Statement	0.4.0.1862.1.4	Fixed

Certificate Policies	This extension includes the following OIDs: 1. The QV Qualified Certificate Class OID = 1.3.6.1.4.1.8024.1.400 2. The QCP Public + SSCD OID (0.4.0.1456.1.1)	Fixed
Adobe Time Stamp (OID = 1.2.840.113583.1.1.9.1)	http://tsa01.quovadisglobal.com/TSS/HttpTspServer	Fixed
Adobe Archive RevInfo (OID = 1.2.840.113583.1.1.9.2)	This relates to OCSP revocation checking within Adobe products for long term validation purposes.	Fixed

10.6.2 Qualified Certificate Profile – Organisation / QCP Public

Qualified certificates issued for natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under the eIDAS Regulation until they expire.

Purpose

The purpose of a Qualified Organisation Digital Certificate is to identify the signatory with a high level of assurance, for the purpose of creating advanced electronic signatures meeting the qualification requirements defined by the applicable legal framework of the Electronic Signatures Directive (1999/93/EC).

Registration Process

Validation procedures for QuoVadis Qualified Organisation Digital Certificates are consistent with the Qualified Certificate Policy (QCP public) policy described in ETSI TS 101 456.

In all cases, an authorized individual is responsible for all aspects of Certificate management and entering into the QuoVadis Certificate Holder Agreement on behalf of the named organisation.

Evidence of the authorized individual's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence.

Evidence shall be provided of:

- Full name of authorized individual (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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.
- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the authorized individual is associated with and authorized by the organisational entity.

Fields	Contents	Demarcation
Subject		
Common Name (CN)	Common Name	Holder Variable
Organisational Unit (OU)	Organisational Unit	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Locality	Holder Variable
State or Province	Not Stipulated	Holder Variable
Country	State or Province	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		Fixed
Key Usage	Non Repudiation	Fixed
QC Statement PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed
QC Statement ETSI Compliance	0.4.0.1862.1.1	Fixed
Certificate Policies	This extension includes the following OIDs: The QV Qualified “QCP Public” OID = 1.3.6.1.4.1.8024.1.450 The ETSI QCP Public OID (0.4.0.1456.1.2)	Fixed

10.7 QV Qualified – SuisseID

Purpose

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Qualified Certificates are used to sign documents electronically. The digital signature is tamperproof and legally equivalent to a handwritten signature.

Either a Common Name or a Pseudonym is required for QuoVadis SuisseID Qualified Certificate. Use of both Common Name and Pseudonym in the same Certificate is not permitted.

Registration Process

QuoVadis SuisseID Qualified Certificates are issued in accordance with the SuisseID requirements (including the "SuisseID Specification" document) using the QuoVadis SuisseID Signing Service. Unless stated otherwise in the SuisseID Specification document, the guidelines in TAV-ZERTES apply to the specification of SuisseID Qualified Certificates.

For the issuance and life cycle management of SuisseID Qualified Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant qualified certificate.

Evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a 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 Certificate Holder is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorization from an authorized Organisation representative; and
- Evidence that the Certificate Holder is associated with the organisational entity.

Private Keys for SuisseID Qualified Certificates are generated and stored on a Hardware Security Module that meets FIPS PUB 140-2, level 3 or EAL 4 standards. This Hardware Security Module is located in a QuoVadis data centre. Access by the Certificate Holder 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.

QuoVadis SuisseID Qualified Certificates have a maximum validity of three years.

Fields	Contents	Demarcation
Signature Algorithm	sha256RSA	
Subject		

Common Name (CN)	First Name - Last Name (Qualified Signature)	Holder Variable
Pseudonym	Pseudonym (Qualified Signature)	Holder Variable
Title	Title (e.g. Dr.) which must be as written in ID Document/ Passport)	Holder Variable
Serial Number	1200-xxxx-xxxx-xxxx	Fixed
Organisational Unit (OU)	Variable Data	Holder Variable
Organisation (O)	Organisation legal name	Holder Variable
Locality	Locality	Holder Variable
State/Province	State/Province	Holder Variable
Country	Country	Holder Variable
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Non Repudiation	Fixed
Certificate Policies		
CertPolicyID (SuisseID)	2.16.756.5.26.1.1.1	Fixed
User Notice	SuisseID qualified certificate	Fixed
CertPolicyID (Public + SSCD)	0.4.0.1456.1.1	Fixed
CertPolicyID (QuoVadis Cert Class)	1.3.6.1.4.1.8024.1.400	Fixed
URL	https://www.quovadisglobal.com/repository	Fixed
Subject Alternative Name		
RFC822 email address	RFC822 email address (same as subject email address)	Holder Variable
Issuer Alternative Name	O= ZertES Recognition Body: KPMG AG	Fixed
qcStatements		
ETSI Compliance	0.4.0.1862.1.1	Fixed
SSCD Statement	0.4.0.1862.1.4	Fixed
PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed

10.8 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.

10.8.1 Grid Certificates

This section provides an overview of the requirements and Digital Certificate contents for Grid Digital Certificates issued in accordance with the requirements of the International Grid Trust Federation (IGTF) or one of its member bodies. The IGTF is the body that is responsible for establishing common policies and guidelines between its member Policy Management Authorities (PMAs). The IGTF consists of the Asia Pacific Grid Policy Management Authority (APGridPMA), the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) and The Americas Grid Policy Management Authority (TAGPMA).

This section (10.6.1) of the CP/CPS relates only to Grid Certificates, which may only be used for Grid related purposes. In relation to Grid Certificates, this section of the CP/CPS will take precedence over the remainder of the CP/CPS if there are any conflicts or contradictions. Major changes to this CP/CPS relating to Grid Digital Certificates will be announced to the relevant Grid PMA and their approval must be gained before Grid Digital Certificates under the new CP/CPS are issued.

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. The QuoVadis Root Certificates are available on the QuoVadis website and also on the TACAR (TERENA Academic CA Repository) trust anchor repository (https://www.tacar.org/repos/).

All Grid Digital 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 Digital Certificates. Revocation requests must be properly authenticated before they are accepted. Revocation requests can be made by end entities, Registration Authorities 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 Digital Certificate, or if the data in the Digital Certificate is no longer valid. Proxy Certificates will be supported in relation to Grid Digital Certificate. A Grid Digital Certificate must be revoked if a related Proxy Certificate is compromised in any way. The maximum Certificate Revocation List lifetime for Grid Digital Certificates is 30 days.

Grid Certificate Re-Keying can only take place if the Certificate Holder 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 Certificate Holder is required to apply for a new Certificate. If the Certificate Holder has lost their Private Key, or if their existing Certificate has expired, they will need to apply for new Certificate.

10.8.1.1 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 Certificate Holder to access the Grid services that require Certificate-based authentication.
Registration Process
The identity vetting of all Applicants must be performed by an approved Registration Authority (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 Digital 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.

Fields	Contents	Demarcation
Issuer		

Common Name (CN)	QuoVadis Grid ICA / QuoVadis Grid ICA G2	Fixed
Organisation (O)	QuoVadis Limited	Fixed
Country (C)	BM	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M (Maximum Digital Certificate lifetime of 1 year)	Fixed
Subject		
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=<organisation identifier>, DC=users	Holder Variable
Common Name (CN)	First Name and Last Name of Certificate Holder (Common Name must be unique)	Holder Variable
Organisational Unit (OU)	Optional	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Locality	Holder Variable
State/Province (ST)	State/Province	Holder Variable
Country (C)	Country	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Digital Signature Key Encipherment Data Encipherment	Fixed
Certificate Policies	1. Certificate Policy (QuoVadis Grid ICA OID): Policy Identifier=1.3.6.1.4.1.8024.0.1.10.0.0 2. Certificate Policy (IGTF Classic Authentication Profile): Policy Identifier=1.2.840.113612.5.2.2.1	Fixed
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	Fixed
Subject Alternative Name	Email Address (RFC 822 Name)	Holder Variable

10.8.1.2 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 Registration Authority (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.

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 Digital Certificate. The RA is responsible for maintaining documented evidence on retaining the same identity over time.

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.

Fields	Contents	Demarcation
Issuer		
Common Name (CN)	QuoVadis Grid ICA / QuoVadis Grid ICA G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Limited	Fixed
Country (C)	BM	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M (Maximum certificate lifetime of 1 year)	Fixed
Subject		
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=< organisation identifier >, DC=hosts	Holder Variable
Common Name (CN)	Subject Common Name	Holder Variable
Organisational Unit (OU)	Organisational Unit	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Locality	Holder Variable
State/Province (ST)	State/Province	Holder Variable

Country (C)	Country	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Digital Signature Key Encipherment Data Encipherment	Fixed
Certificate Policies	3. Certificate Policy (QuoVadis Grid ICA OID): Policy Identifier=1.3.6.1.4.1.8024.0.1.10.0.0 4. Certificate Policy (IGTF Classic Authentication Profile OID): Policy Identifier=1.2.840.113612.5.2.2.1	Fixed
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Fixed
Subject Alternative Name	SAN dNSName with the Fully Qualified Domain Name or an iPAddress	Holder Variable

10.9 QuoVadis Device

Purpose

QuoVadis Device Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. QuoVadis Device Certificates (i.e. with the OID 1.3.6.1.4.1.8024.1.600 in Certificate Policies) that have the Server Authentication Extended Key Usage comply with the CA/B Forum Baseline Requirements.

Device 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.

Registration Process

QuoVadis acts as Registration Authority (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 Certificate Holder Agreement for the requested Certificate.

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. QuoVadis may also use the services of a third party to confirm Applicant information.

High Risk Domains

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

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.

Fields	Contents	Demarcation
Issuer		
Common Name (CN)	QuoVadis Grid ICA / QuoVadis Grid ICA G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Limited	Fixed
Country (C)	BM	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M (Maximum certificate lifetime of 1 year)	Fixed
Subject		
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=< organisation identifier >, DC=hosts	Holder Variable
Common Name (CN)	Subject Common Name	Holder Variable
Organisational Unit (OU)	Organisational Unit	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Locality	Holder Variable
State/Province (ST)	State/Province	Holder Variable
Country (C)	Country	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Depends on the type of certificate.	Holder Variable

Extended Key Usage	Depends on the type of certificate. May include (where relevant): • Server Authentication (1.3.6.1.5.5.7.3.1) • Client Authentication (1.3.6.1.5.5.7.3.2) • Time Stamping (1.3.6.1.5.5.7.3.8) • Secure Email (1.3.6.1.5.5.7.3.4) • Smart Card Logon (1.3.6.1.4.1.311.20.2.2) • Code Signing (1.3.6.1.5.5.7.3.3) • KDC Authentication (1.3.6.1.5.2.3.5)	Holder Variable
Subject Alternative Name	If the Server Authentication 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.	Holder Variable
Certificate Policies	This extension includes the QV Device Certificate Class OID = 1.3.6.1.4.1.8024.1.600. If the Server Authentication EKU is present: = 2.23.140.1.2.2 If the Server Authentication 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) If the Code Signing EKU is present: = 2.23.140.1.2.3	Fixed
Certificate Transparency (optional)	(1.3.6.1.4.1.11129.2.4.4) If the Server Authentication EKU is present, this field MAY include two or more Certificate Transparency proofs from approved CT Logs.	

11 APPENDIX B

11.1 Business SSL

Field	Value
Version	V3
Serial Number	Unique number
Issuer Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis QVRCA1G1 SSL ICA or QuoVadis QVRCA1G3 SSL ICA or QuoVadis QVRCA3G1 SSL ICA or QuoVadis QVRCA3G3 SSL ICA O = QuoVadis Limited C = BM
Validity Period	1, 2, or 3 years expressed in UTC format
Subject Distinguished Name	
Organization Name	subject:organisationName (2.5.4.10)
Organisation Unit	subject:organisationUnit (2.5.6.5) Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)
Country	subject:countryName (2.5.4.6)
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)
Extension	**Value**
Authority Key Identifier	c=no; Octet String – Same as Issuer's Subject Key Identifier
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1)

	Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository
Certificate Transparency (optional)	(1.3.6.1.4.1.11129.2.4.4) This field MAY include two or more Certificate Transparency proofs from approved CT Logs.

Purposes of Business SSL

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

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

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

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

Eligible Applicants

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

Verification Requirements

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

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

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

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

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

a) the IP Address range assignment by country for either (i) the web site's IP
b) address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;
c) the ccTLD of the requested Domain Name;
d) information provided by the Domain Name Registrar; or
e) a method identified in "Identity" above.

Application Process

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

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

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

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

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

Step 6: QuoVadis creates the Business SSL Certificate.

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

Renewal

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

11.2 Code Signing

Field	Value	Comments
Version	V3	
Serial Number	Unique number	
Issuer Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	
Issuer Distinguished Name	Issuer Distinguished Name	
Validity Period	1, 2, or 3 years expressed in UTC format	
Subject Distinguished Name		
Organization Name	subject:organisationName (2.5.4.10)	Required field. The Subject's verified legal name.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Optional field. Must not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless QuoVadis has verified this information
Common Name	subject:commonName (2.5.4.3)	Required field. The Subject's verified legal name.
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	Required if the subject:localityName field is absent. Optional if the

		subject:localityName fields is present.
Locality	subject:locality (2.5.4.6)	Required if the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field is present.
Country	subject:countryName (2.5.4.6)	Required field.
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	

Extension	Value
Authority Key Identifier	c=no; Octet String
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; Digital Signature (80)
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codesSigning)

Field	Value	Comments
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; { 2.23.140.1.4.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository	1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID. 2.23.140.1.2.3 is the Code Signing Minimum Requirements OID.
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =http://ocsp.quovadisglobal.com - id-ad-caIssuers (Certification Authority Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/<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 organizations, trade associations, and other entities.

Private Key Protection

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

- A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Certificate
- Holder’s private key protection through a TPM key attestation
- A hardware cryptographic module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
- Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Certificate Holder MUST also warrant that it will

keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Verification Requirements

Before issuing a Code Signing Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to sign code in the name to be included in the Certificate.

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

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

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

1. Verifies the Subject's identity using a government photo ID,
2. Verifies the Subject's address using reliable data sources,
3. Obtains a biometric associated with the Subject, such as a fingerprint or notarized handwritten Declaration of Identity,
4. Verifies the Certificate Requester's authority to request a certificate and the authenticity of the Certificate request using a verified method of communication.

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

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

Application Process

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

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

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

Step 3: The Applicant accepts the Certificate Holder Agreement and approves Certificate issuance.

Step 4: All signatures are verified through follow-up procedures or telephone calls.

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

Step 6: QuoVadis creates the Code Signing Certificate. Step 7: The Certificate is delivered to the Applicant.

12 APPENDIX C

12.1.1 Definitions and Acronyms

In this QuoVadis CP/CPS the following Key terms and Abbreviations shall have the following meaning in the operation of the QuoVadis PKI unless context otherwise requires:

"**Advanced Electronic Signature**" means an electronic signature which meets the requirements set out in Article 26 of the eIDAS Regulation.

"**Applicant**" means an Individual or Organisation that has submitted an application for the issue of a Digital Certificate.

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

"**Approved Client Issuing CA**" means an Issuing CA managed and operated by an external third party.

"**Authorised Relying Party**" means an Individual or Organisation that has entered into a Relying Party Agreement authorizing that person or Organisation to exercise Reasonable Reliance on Digital Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

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

"**Authentication**" means the procedures and requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to provide against fraud, imitation and deception ("Authenticate" and "Authenticated" to be construed accordingly).

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

"**Certificate Application**" Any of several forms completed by Applicant or QuoVadis and used to process the request for an EV Certificate, including but not limited to

agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

"**Certification**" means the process of creating a Digital Certificate for an entity and binding that entity's identity to the Digital Certificate.

"**Certification Authority**" means an entity trusted by one or more entities to create, assign or revoke Digital Certificates.

"**Certification Authority Officer**" means a responsible person, in a trusted role, who is involved in the day-to-day operations of a Certification Authority.

"**CP/CPS**" is a publicly available document that details the QuoVadis PKI and describes the practices employed in issuing Digital Certificates.

"**Certificate Holder**" means a Holder of a Digital Certificate chained to the QuoVadis Root Certificate, including without limitation, organisations, individuals and/or hardware and/or software devices. A Certificate Holder is (i) named in a Digital Certificate or responsible for the Device named in a Digital Certificate and (ii) holds a Private Key corresponding to the Public Key listed in that Digital Certificate. Certificate Holder in the context of an TLS/SSL Certificate means either the Individual to whom an end entity Certificate is issued, referred to as a Registrant in the Trust/Link system or the Individual responsible for requesting, installing and maintaining the trusted system for which an SSL Certificate has been issued, referred to as a Subscriber in the Trust/Link system.

"**Certificate Holder Agreement**" means a contract between a Certificate Holder and an Issuing Certification Authority that contains, expressly or by reference, the terms and conditions of use within the QuoVadis PKI. In the context of the itsme Issuing CA G1 the Certificate Holder Agreement is referred to as the Terms and Conditions.

"**Certificate Chain**" means a chain of Digital Certificates required to validate a Holder's Digital Certificate back through its respective Issuing Certification Authority to the Root Certification Authority.

"**Certificate Policy**" means a certificate policy adopted by an Issuing Certificate Authority operating within the QuoVadis PKI that defines all associated rules and indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

"**Certificate Renewal**" is when all the identifying information and the Public Key from the old certificate are duplicated in the new certificate, but there is a different (longer) validity period.

"**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.

"**Certificate Re-issuance**" is when a Certificate Holder registers for a new certificate, but there is an opportunity to change the identifying information (e.g. new email address, new last name, etc.) or other information (corrected certificate policies, modified key usage, etc.) from what was in the old certificate. The new certificate also has a different Public Key and a different validity period from the old certificate.

"**Certificate Re-key**" is when all the identifying information from the old certificate is duplicated in the new certificate, but there is a different Public Key and a different validity period.

"**Certificate Revocation**" means the process of removing a Digital Certificate from the management system and indicating that the Key Pair related to that Digital Certificate should no longer be used.

"**Certificate Revocation List**" means a list of Digital Certificates signed by the Issuing Certification Authority that have been revoked.

"**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**" is a natural person who is employed by the Applicant and who has express authority to sign Certificate Holder Agreements on behalf of the Applicant.

"**Counterparty**" means a person that is known to a Nominating Registration Authority or its respective Subsidiaries or Holding Companies and where the relationship with the Counterparty was established in accordance with recognised and documented Know Your Customer standards and with whom the Registration Authority is reliably able to identify the Counterparty through business records maintained by the Registration Authority or obtained from its respective Subsidiaries or Holding Companies.

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

"**Digital Certificate**" means 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 Digital 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.

"**Digital Signature**" means data appended to, or a cryptographic transmission of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit.

"**Digital Transmission**" means the transmission of information in an electronic format.

"**Device**" means software, hardware or other electronic or automated means configured to act in a particular way without human intervention.

"**Device Certificate**" means a Digital Certificate issued to identify a Device.
"Distinguished Name" means the unique identifier for the Holder of a Digital Certificate.

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

"**Enterprise RA**" means an employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organisation.

"**EU Qualified Certificate**" means qualified certificate as specified in Regulation (EU) No 910/2014.

"**Federal Information Processing Standards**" (FIPS) means the standards that deal with a wide range of computer system components including: hardware, storage media, data files, codes, interfaces, data transmission, networking, data management, documentation, programming languages, software engineering, performance and security.

"**Identify**" means a process to distinguish a subject or entity from other subjects or entities.

"**Identity**" means a set of attributes which together uniquely identify a natural person or entity.

"**Identification**" means reliance on data to distinguish and Identify a natural person or entity.

"**Individual**" means a natural person.

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

"**Issuing Certification Authority**" ("Issuing CA") means a Certification Authority duly authorised to operate by QuoVadis to issue Digital Certificates to Certificate Holders within the QuoVadis PKI.

"**Issuing CA Agreement**" an agreement entered into between QuoVadis and an Issuing CA to provide Issuing CA services within the QuoVadis PKI.

"**Issuing CA Certificate**" A Digital Certificate issued by the QuoVadis Root Certification Authority to an Issuing CA enabling that Issuing CA to issue Digital Certificates to Certificate Holders.

"**Key**" means a sequence of symbols that controls the operation of a cryptographic transformation (e.g. Encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

"**Key Pair**" means two related Keys, one being a Private Key and the other a Public Key having the ability whereby one of the pair will decrypt the other.

"**Object Identifier**" means the unique identifier registered under the ISO registration standard to reference a specific object or object class.

"**Operational Term**" means the term of validity of a Digital Certificate commencing on the date of its issue and terminating on the earlier of (i) the date disclosed in that Digital Certificate or (ii) the date of that Digital Certificate's Revocation.

"**Organisation**" means an entity that is legally recognised in its jurisdiction of domicile (and can include a body corporate or un-incorporate, partnership, trust, non-profit making Organisation, or Government entity).

"**Participants**" means participants within the QuoVadis PKI and include (i) Issuing CAs and their Subsidiaries and Holding Companies; (ii) Registration Authorities and their Subsidiaries and Holding Companies; (iii) Certificate Holders, (including Certificate Applicants); (iv) Authorised Relying Parties.

"**PKCS**" means Public-Key Cryptography Standard.

"**Policy Management Authority**" means the QuoVadis body responsible for overseeing and approving CP/CPS amendments and general management.

"**Proprietary Marks**" means any patents (pending or otherwise), trade marks, trade names, logos, registered designs, symbols, emblems, insignia, fascia, slogans, copyrights, know-how, information, drawings, plans and other identifying materials whether or not registered or capable of registration and all other proprietary rights whatsoever owned by or available to QuoVadis adopted or designated now or at any time hereafter by QuoVadis for use in connection with the QuoVadis PKI.

"**Private Key**" means a Key forming part of a Key Pair that is required to be kept secret and known only to the person that holds it.

"**Public Key**" means a Key forming part of a Key Pair that can be made public.

"**Public Key Infrastructure**" (PKI) means a system for publishing the Public Key values used in public key cryptography. Also a system used in verifying, enrolling, and certifying users of a security application.

"**Qualified Certificate**" A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the

qualification requirements defined by the applicable legal framework of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation").

"**Qualified Certificate for Electronic Signature**" means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of Regulation (EU) No 910/2014.

"**Qualified Electronic Signature**" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

"**Qualified Electronic Signature Creation Device**" (QSCD) means an electronic signature creation device that meets the requirements laid down in Annex II of Regulation (EU) No 910/2014.

"**Qualified Trust Service Provider**" (QTSP) means a trust service provider who provides one or more qualified trust services and is granted the qualified status under regulation EU910/2014 by the supervisory body.

"**QuoVadis**" means QuoVadis Limited, a Bermuda exempted company.

"**QuoVadis Issuing Certification Authority**" means QuoVadis in its capacity as an Issuing CA.

"**QuoVadis PKI**" means the infrastructure implemented and utilised by QuoVadis for the generation, distribution, management and archival of Keys, Digital Certificates and Certificate Revocation Lists and the Repository to which Digital Certificates and Certificate Revocation Lists are to be posted.

"**QuoVadis Root Certification Authority**" means QuoVadis in its capacity as a Root Certification Authority.

"**QSCD**" means Qualified electronic Signature/Seal Creation Device

"**Registration Authority**" means a Registration Authority designated by an Issuing CA to operate within the QuoVadis PKI responsible for identification and authentication of Certificate Holders.

"**Registration Authority Agreement**" an agreement entered into between an Issuing CA and a Registration Authority pursuant to which that Registration Authority is to provide its services within the QuoVadis PKI.

"**Registration Authority Certificate**" means a digital identifier issued by an Issuing CA (including QuoVadis in its capacity as an Issuing CA) in connection with the establishment of a Registration Authority within the QuoVadis PKI.

“**Registration Authority Officer**” means an Individual designated by a Registration Authority as being authorised to perform the functions of that Registration Authority.

“**Regulated Certificate**” means a Digital Certificate that meets the requirements of Article 7 of ZertES (see section 8.1.1).

“**Regulated electronic signature**” means 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**” means 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**” means a party that acts in reliance on a Digital Certificate. Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued. Certificate Holder is not required to ensure that potential relying parties are compliant with the requirements to be an Authorised Relying Party.

“**Relying Party Agreement**” sets forth the terms and conditions under which an Individual or Organisation is entitled to exercise Reasonable Reliance on Digital Certificates.

“**Repository**” means one or more databases of Digital Certificates and other relevant information maintained by Issuing CAs.

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

“**Reserved IP Address**” means an IPv4 or IPv6 address that the IANA has marked as reserved.

“**Root Certification Authority Certificate**” means the self-signed Digital Certificate issued to the QuoVadis Root Certification Authority.

“**Root Certification Authority**” means QuoVadis as the source Certification Authority being a self-signed Certification Authority that signs Issuing CA Certificates.

"**Secure Cryptographic Device**" means device which holds the Certificate Holder's private key, protects this key against compromise and performs signing or decryption functions on behalf of the Certificate Holder.

"**Secure Signature Creation Device**" (SSCD) means a secure container specifically designed to carry and protect a digital certificate, which meets the following requirements laid down in annex III of Directive 1999/93/EC:

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
   a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
   b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
   c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

"**Subordinate CA**" means a Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

"**Subscriber**" means a natural or legal person that has entered a formal contract with QuoVadis for the issuance of Digital Certificates to Certificate Holders. The Subscriber may be responsible for the identity vetting of these Certificate Holders. A Subscriber may also hold a Digital Certificate (but is not required to).

"**Technically Constrained Subordinate CA Certificate**" means 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.

"**Token**" means a Cryptographic Module consisting of a hardware object (e.g., a "smart card"), often with a memory and microchip.

"**Utility Certificate**" means a Digital Certificate issued to a Responsible Person/s to be used in the day-to-day administration of the QuoVadis PKI.

"**Validation**" means an online check, by Online Certificate Status Protocol request, or a check of the applicable Certificate Revocation List(s) (in the absence of Online Certificate Status Protocol capability) of the validity of a Digital Certificate and the validity of any Digital Certificate in that Digital Certificate's Certificate Chain for the purpose of confirming that the Digital Certificate is valid at the time of the check (i.e., it is not revoked or expired).

Acronyms

CA	Certificate Authority or Certification Authority
CAA	Certificate Authority Authorisation
CP/CPS	Certificate Policy & Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
PMA	QuoVadis Policy Management Authority
EV	Extended Validation
FIPS	Federal Information Processing Standard
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ERA	Enterprise Registration Authority
LRA	Local Registration Authority
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework