QuoVadis Trust Anchor Root Certification Authority

Certification Policy/ Certification Practice Statement

OIDs:	1.3.6.1.4.1.8024.0.4
Effective Date:	March 7, 2016
Version:	1.0

This CPS applies to all entities participating in or using the QuoVadis Private PKI services, which are not publicly trusted. Certificates issued out of this service are signed by the QuoVadis Trust Anchor Root Certification Authority and are not subject to the audit and compliance requirements of the CA/Browser Forum or software/application vendors.

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 Private 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 Private PKI that relate to all CAs established by QuoVadis under the QuoVadis Trust Anchor Root Certification Authority.

Contact Information

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

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

Website: www.quovadisglobal.com

e-mail: compliance@quovadisglobal.com

Version Control

Author	Date	Version	Comment
QuoVadis PMA	07 March 2016	1.00	First version

TABLE OF CONTENTS

1.1. Overview 1
1.2. Document Name, Identification and Applicability 2
1.3. Public Key Infrastructure Participants 2
1.3.1. Certification Authorities 3
1.3.2. Registration Authorities and Their Obligations 5
1.3.3. Certificate Holders 5
1.3.4. Relying Parties 6
1.3.5. Other Participants 7
1.4. Certificate Usage 8
1.4.1. Appropriate Certificate Usage 8
1.4.2. Prohibited Certificate Usage 8
1.5. Policy Administration 8
1.5.1. Organisation Administering the CP/CPS 8
1.5.2. Contact Person 8
1.5.3. Person Determining the CP/CPS Suitability 8
1.5.4. CP/CPS Approval Procedures 9
1.6. Definitions and Acronyms 9
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 9
2.1. Repositories 9
2.2. Publication of Certificate Information 9
2.3. Time or Frequency of Publication 9
2.4. Access Controls on Repositories 9
3. IDENTIFICATION AND AUTHENTICATION 9
3.1. Naming 10
3.1.1. Types Of Names 10
3.1.2. Need For Names To Be Meaningful 10
3.1.3. Pseudonymous Certificate Holders 10
3.1.4. Rules For Interpreting Various Name Forms 10
3.1.5. Uniqueness Of Names 11
3.1.6. Recognition, Authentication, And Role Of Trademarks 11
3.2. Initial Identity Validation 11
3.2.1. Method To Prove Possession Of Private Key 11
3.2.2. Authentication Of Organisation Identity 11
3.2.3. Authentication Of Individual Identity 11
3.2.4. Non-Verified Certificate Holder Information 11
3.2.5. Validation Of Authority 11
3.2.6. Criteria For Interoperation 11
3.3. Identification And Authentication For Renewal Requests 11
3.3.1. Identification and Authentication For Routine Re-Key 11
3.3.2. Identification and Authentication For Re-Key After Revocation 11
3.4. Identification and Authentication For Revocation Requests 12
3.4.1. Issuing Certification Authority 12
3.4.2. Registration Authority 12
3.4.3. Certificate Holder 12
4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS 12
4.1. Certificate Application 12
4.1.1. Who Can Submit A Certificate Application 12
4.1.2. Enrolment Process And Responsibilities 12
4.2. Certificate Application Processing 13
4.2.1. Performing Identification And Authentication Functions 13
4.2.2. Approval Or Rejection Of Certificate Applications 13
4.2.3. Time To Process Certificate Applications 13
4.2.4. Certificate Authority Authorisation (CAA) 13
4.3. Certificate Issuance 13

4.3.1. Certification Authority Actions During Certificate Issuance....13
4.3.2. Notification To Applicant Certificate Holder By The Certification Authority Of Issuance Of Certificate....14
4.4. Certificate Acceptance....14
4.4.1. Notice Of Acceptance....14
4.4.2. Conduct Constituting Certificate Acceptance....15
4.4.3. Publication Of The Certificate By The Certification Authority....15
4.4.4. Notification Of Certificate Issuance By The Certification Authority To Other Entities....15
4.5. Key Pair And Certificate Usage....15
4.5.1. Certificate Holder Private Key And Certificate Usage....15
4.5.2. Relying Party Public Key And Certificate Usage....15
4.6. Certificate Renewal....15
4.7. Certificate Re-Key....16
4.7.1. Circumstance For Certificate Re-Key....16
4.7.2. Who May Request Re-Key....16
4.7.3. Processing Certificate Re-Key Request....16
4.7.4. Notification Of New Certificate Issuance To Certificate Holder....16
4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate....16
4.7.6. Notification Of Certificate Re-Key By The Certification Authority To Other Entities....16
4.8. Certificate Modification....16
4.9. Certificate Revocation And Suspension....17
4.9.1. Circumstances For Revocation....17
4.9.2. Who Can Request Revocation....18
4.9.3. Procedure For Revocation Request....18
4.9.4. Revocation Request Grace Period....18
4.9.5. Time Within Which The Certification Authority Must Process The Revocation Request....18
4.9.6. Revocation Checking Requirement For Relying Parties....18
4.9.7. Certificate Revocation List Issuance Frequency....18
4.9.8. Maximum Latency For Certificate Revocation List....19
4.9.9. On-Line Revocation/Status Checking Availability....19
4.9.10. On-Line Revocation Checking Requirement....19
4.9.11. Other Forms Of Revocation Advertisements Available....19
4.9.12. Special Requirements in Relation to Key Compromise....19
4.9.13. Circumstances For Suspension....19
4.9.14. Who Can Request Suspension....19
4.9.15. Procedure For Suspension Request....19
4.9.16. Limits On Suspension Period....19
4.10. Certificate Status Services....19
4.10.1. Operational Characteristics....19
4.10.2. Service Availability....19
4.10.3. Optional Features....19
4.11. End Of Subscription....19
4.12. Key Archival And Recovery....20
4.12.1. Key Archival And Recovery Policy And Practices....20
4.12.2. Session Key Encapsulation And Recovery Policy And Practices....20
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS....20
5.1. Physical Controls....20
5.1.1. Site Location and construction....20
5.1.2. Physical Access....20
5.1.3. Power and Air-Conditioning....21
5.1.4. Water Exposures....21
5.1.5. Fire Prevention and Protection....21
5.1.6. Media Storage....21
5.1.7. Waste Disposal....21
5.1.8. Off-Site Backup....21
5.2. Procedural Controls....21

5.2.1. Trusted Roles 22
5.2.2. Number of Persons Required Per Task 22
5.2.3. Identification and Authentication For Each Role 22
5.2.4. Roles Requiring Separation of Duties 22
5.3. Personnel Controls 22
5.3.1. Qualifications, Experience, and Clearance Requirements 23
5.3.2. Background Check Procedures 23
5.3.3. Training Requirements 23
5.3.4. Retraining Frequency And Requirements 23
5.3.5. Job Rotation Frequency And Sequence 23
5.3.6. Sanctions for Unauthorised Actions 23
5.3.7. Independent Contractor Requirements 23
5.3.8. Documentation Supplied To Personnel 23
5.4. Audit Logging Procedures 24
5.4.1. Types Of Events Recorded 24
5.4.2. Frequency Of Processing Log 24
5.4.3. Retention Period For Audit Log 24
5.4.4. Protection Of Audit Log 24
5.4.5. Audit Log Backup Procedures 24
5.4.6. Audit Collection System 25
5.4.7. Notification To Event-Causing Subject 25
5.4.8. Vulnerability Assessment 25
5.5. Records Archival 25
5.5.1. Types Of Records Archived 25
5.5.2. Retention Period For Archive 25
5.5.3. Protection Of Archive 25
5.5.4. Archive Backup Procedures 26
5.5.5. Requirements For Time-Stamping Of Records 26
5.5.6. Archive Collection System 26
5.5.7. Procedures To Obtain And Verify Archive Information 26
5.6. Key Changeover 26
5.7. Compromise And Disaster Recovery 26
5.7.1. QuoVadis Business Continuity Plan 26
5.8. Certification Authority And/Or Registration Authority Termination 27
5.8.1. User Keys And Certificates 27
5.8.2. Successor Issuing Certification Authority 27
6. TECHNICAL SECURITY CONTROLS 27
6.1. Key Pair Generation And Installation 27
6.1.1. Key Pair Generation 27
6.1.2. Private Key Delivery To Certificate Holder 28
6.1.3. Public Key Delivery To Certificate Issuer 28
6.1.4. Certification Authority Public Key To Relying Parties 28
6.1.5. Key Sizes 28
6.1.6. Public Key Parameters Generation And Quality Checking 28
6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field) 29
6.2. Private Key Protection And Cryptographic Module Engineering Controls 29
6.2.1. 6.2.1. Cryptographic Module Standards And Controls 29
6.2.2. Private Key (N Out Of M) Multi-Person Control 29
6.2.3. Private Key Escrow 29
6.2.4. Private Key Backup 29
6.2.5. Private Key Archive 29
6.2.6. Private Key Transfer Into Or From A Cryptographic Module 30
6.2.7. Private Key Storage On Cryptographic Module 30
6.2.8. Method Of Activating Private Key 30
6.2.9. Method Of Deactivating Private Key 30
6.2.10. Method Of Destroying Private Key 30

6.2.11. Cryptographic Module Rating 30
6.3. Other Aspects Of Key Pair Management 30
6.3.1. Public Key Archival 30
6.3.2. Certificate Operational Periods And Key Pair Usage Periods 30
6.4. Activation Data 31
6.4.1. Activation Data Generation And Installation 31
6.4.2. Activation Data Protection 31
6.4.3. Other Aspects Of Activation Data 31
6.5. Computer Security Controls 31
6.5.2. Computer Security Rating 31
6.6. Life Cycle Technical Controls 32
6.6.1. System Development Controls 32
6.6.2. Security Management Controls 32
6.6.3. Life Cycle Security Controls 32
6.7. Network Security Controls 32
7. CERTIFICATE, CRL, AND OCSP PROFILES 32
7.1. Certificate Profile 32
7.1.1. Basic Certificate Contents 33
7.1.2. Certificate Extensions 33
7.1.3. Algorithm Object Identifiers 35
7.1.4. Name Forms 35
7.1.5. Name Constraints 35
7.1.6. CP/CPS Object Identifier 35
7.1.7. Usage Of Policy Constraints Extension 35
7.1.8. Policy Qualifiers Syntax And Semantics 35
7.1.9. Processing Semantics For The Critical Certificate Policies Extension 35
7.2. Certificate Revocation List Profile 35
7.2.1. Version Number 36
7.2.2. Certificate Revocation List And Certificate Revocation List Entry Extensions 36
7.3. Online Certificate Status Protocol Profile 36
7.3.1. Online Certificate Status Protocol Version Numbers 36
7.3.2. Online Certificate Status Protocol Extensions 36
7.4. Lightweight Directory Access Protocol Profile 36
7.4.1. Lightweight Directory Access Protocol Version Numbers and Lightweight Directory Access Protocol Extensions 36
7.5. Digital Certificate Fields and Root CA Certificate Hashes 37
7.5.1. Digital Certificate Fields 37
7.5.2. QuoVadis Root Certificate Hashes 38
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 38
8.1. Frequency, Circumstance And Standards Of Assessment 38
8.1.1. QuoVadis Certification Authority 38
9. OTHER BUSINESS AND LEGAL MATTERS 38
9.1. Fees 38
9.1.1. Certificate Issuance Or Renewal Fees 38
9.1.2. Certificate Access Fees 38
9.1.3. Revocation Or Status Information Access Fees 39
9.1.4. Fees For Other Services 39
9.1.5. Refund Policy 39
9.2. Financial Responsibilities 39
9.2.1. Insurance Coverage 39
9.2.2. Other Assets 39
9.2.3. Insurance Or Warranty Coverage For End-Entities 39
9.2.4. Fiduciary Relationships 39
9.3. Confidentiality Of Business Information 40
9.3.1. Scope Of Confidential Information 40
9.3.2. Information Not Within The Scope Of Confidential Information 40

9.3.3. Responsibility To Protect Confidential Information....40
9.4. Privacy Of Personal Information....40
9.4.1. Privacy Plan....40
9.4.2. Information Treated As Private....40
9.4.3. Information Deemed Not Private....41
9.4.4. Responsibility To Protect Private Information....41
9.4.5. Notice And Consent To Use Private Information....41
9.4.6. Disclosure Pursuant To Judicial Or Administrative Process....41
9.4.7. Other Information Disclosure Circumstances....42
9.5. Intellectual Property Rights....42
9.5.1. Object Identifiers....42
9.5.2. Licences....42
9.5.3. IETF Guidelines....42
9.5.4. Breach....42
9.6. Representations And Warranties....42
9.6.1. Certification Authority Representations....42
9.6.2. Registration Authority Representations and Warranties....43
9.6.3. Certificate Holder Representations And Warranties....43
9.6.4. Relying Parties Representations And Warranties....44
9.6.5. Representations And Warranties Of Other Participants....44
9.7. Disclaimers Of Warranties....44
9.8. Liability and Limitations of Liability....44
9.8.1. QuoVadis Liability....44
9.8.2. QuoVadis' Limitations Of Liability....44
9.8.3. Excluded Liability....45
9.8.4. Mitigation Of QuoVadis' Liability....46
9.8.5. Claims Against QuoVadis Liability....46
9.9. Indemnities....46
9.10. Term And Termination....47
9.10.1. Term....47
9.10.2. Termination....47
9.10.3. Effect Of Termination And Survival....47
9.11. Individual Notices And Communications With Participants....47
9.12. Amendments....47
9.12.1. Procedure For Amendment....47
9.12.2. Notification Mechanism And Period....47
9.12.3. Circumstances Under Which Object Identifiers Must Be Changed....48
9.13. Dispute Resolution Provisions....48
9.14. Governing Law....48
9.15. Compliance With Applicable Law....48
9.16. Miscellaneous Provisions....48
9.16.1. Entire Agreement....48
9.16.2. Assignment....48
9.16.3. Severability....48
9.16.4. Enforcement (Attorneys' Fees And Waiver Of Rights)....48
9.16.5. Force Majeure....49
9.17. Other Provisions....49
10. APPENDIX A....49
10.1. Digital Certificate Profiles....49
10.1.1. QuoVadis Certificate Class....49
10.2. QV Trust Anchor End User....49
10.3. QV Trust Anchor Device....50
11. APPENDIX B....51
11.1. Definitions and Acronyms....51

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 Private PKI.

This CP/CPS outlines the trustworthiness and integrity of the operations relating to the QuoVadis Trust Anchor Root CAs (QVTARCA) operations. A fundamental concept underpinning the operation of the QuoVadis Private 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.

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

- WebTrust for Certification Authorities, conducted by Ernst & Young. This audit is consistent with standards promulgated by the American National Standards Institute, the Internet Engineering Task Force, and other bodies. It references the ANSI X9.79 Public Key Infrastructure Practices and Policy Framework (X9.79) standard for the financial services community and the American Bar Association's Public Key Infrastructure Assessment Guidelines.
- Qualified Certification Service Provider (Switzerland and Netherlands) entitled to issue and administer Qualified Certificates, conducted by KPMG AG. This includes certification to SR 943.03 (ZertES), ETSI TS 101 456 (Policy requirements for Digital Certification Authorities issuing Qualified Digital Certificates) and other standards.
- 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 PKI Overheid. PKI Overheid 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 PKI Overheid, which can be found in the QuoVadis Repository on the QuoVadis website (http://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.

The detailed provisions of these standards as relates to appropriate certificate content and vetting requirements are not applicable for certificates issued under the QVTARCA, however the general principles of security and certificate lifecycle management are adhered to for all certificates issued by QuoVadis.

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 Private PKI. This CP/CPS merely provides a general overview of the QuoVadis Private PKI including Digital Certificate Profiles as defined in Appendix A.

The QuoVadis Private 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 Private PKI must do so pursuant to definitive contractual documentation.

This CP/CPS undergoes a regular review process and is subject to amendment 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 Private PKI refers to policies contained in the current and in-force CP/CPS.

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 Trust Anchor Root CA and QuoVadis Trust Anchor Root CA G2 1.3.6.1.4.1.8024.0.4

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 Trust Anchor Root CA represents the apex of the QuoVadis Private PKI. The QuoVadis Trust Anchor 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 B.

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 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 Trust Anchor Root CA, i.e. that are within the QuoVadis "chain of trust".

Participants ("Participants") within the QuoVadis Private 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 Private 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 SSL/TLS 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 Private 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 Private PKI contains the following Root Certificates:

SHA1 Roots	**SHA256 Roots**
QuoVadis Trust Anchor Root CA	QuoVadis Trust Anchor Root CA G2

This CP/CPS relates to all generations of the QuoVadis Trust Anchor Root CA.

QuoVadis is obligated to operate the QuoVadis Trust Anchor Root CA, QuoVadis Trust Anchor 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 Private 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.

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 Private 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.

Issuing CAs are required to ensure that all aspects of the services they offer and perform within the QuoVadis Private 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.
- 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.

1.3.1.5. Approved Client Issuing CAs and Their Obligations

An Organisation wishing to participate in the QuoVadis Private 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;
- 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.
- Follow a privacy policy in accordance with this CP/CPS and the applicable Registration Authority Agreement.

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, 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.
- 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.
- 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 Private 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 Private PKI has been compromised.

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 Private 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 Private 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 Private PKI.

1.4. CERTIFICATE USAGE

At all times, participants in the QuoVadis Private 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.

1.4.2. Prohibited Certificate Usage

Digital Certificates may not be used and no participation is permitted in the QuoVadis Private PKI (i) in circumstances that breach, contravene, or infringe the rights of others or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order or (iii) in connection with fraud, pornography, obscenity, hate, defamation 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	Website:	http://www.quovadisglobal.com
QuoVadis Limited	Electronic mail:	compliance@quovadisglobal.com
Suite 1640,		
48 Par-La-Ville Road,		
Hamilton HM-11, Bermuda		

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 Private 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) must 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 http://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 http://www.quovadisglobal.com/repository are available only to Participants in the QuoVadis Private PKI where deemed necessary.

1.6. DEFINITIONS AND ACRONYMS

See Appendix B.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

The QuoVadis Repository (http://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 Private PKI.

2.2. PUBLICATION OF CERTIFICATE INFORMATION

The QuoVadis Trust Anchor 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 to this CP/CPS.

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

There are no specified Identification and authentication procedures for issuance of certificates under the QVTARCA, except that:

Certificates may not be issued with Organisation or Domain Names which are misleading, attempt to convey authority which does not exist or breach the intellectual property rights of an individual or entity whether

registered or not. QuoVadis does not prevent issuance of multiple certificates with the same Subject Distinguished Name and the certificate holder accepts the risk that a certificate to the holder may contain the same subject information as a certificate issued to a different certificate holder.

3.1. NAMING

This section 3.1 outlines best practice for the naming of certificate fields. Participants in the QuoVadis Private PKI should take note of these best practices and endeavour to comply in so far as is practical.

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 Trust Anchor 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 common name of the Certificate Holder. Each User should 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.

3.1.2. Need For Names To Be Meaningful

Distinguished Names should be meaningful, unambiguous and unique. 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 should 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, 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 is in compliance with this CP/CPS and the Digital Certificate Profiles detailed in Appendix A.

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

Not applicable for the QuoVadis Private PKI

3.2.3. Authentication Of Individual Identity

Not applicable for the QuoVadis Private PKI

3.2.4. Non-Verified Certificate Holder Information

Not applicable for the QuoVadis Private PKI

3.2.5. Validation Of Authority

Not applicable for the QuoVadis Private PKI

3.2.6. Criteria For Interoperation

Not applicable for the QuoVadis Private PKI

3.3. IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS

Not applicable for the QuoVadis Private PKI

3.3.1. Identification and Authentication For Routine Re-Key

Not applicable for the QuoVadis Private PKI

3.3.2. Identification and Authentication For Re-Key After Revocation

Not applicable for the QuoVadis Private PKI

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:

- 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 or password 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) a Key Pair for the Digital Certificate is to be generated in a secure fashion, (ii) the binding of the Key Pair to the Digital Certificate shall occur as set forth in this CP/CPS, and (iii) the Issuing CA shall enter into contractual relations with the Certificate Holder for the use of that Digital Certificate and the QuoVadis Private 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. 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 Private 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 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.

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 Private PKI are under no obligation to process Digital Certificate Applications other than within a commercially reasonable time.

4.2.4. Certificate Authority Authorisation (CAA)

QuoVadis does not check for Certification Authority Authorisation (CAA) DNS records (RFC 6844) when issuing Digital Certificates. If alerted to the presence of a CAA record for a Domain, QuoVadis will perform additional verification of the Applicant's authority to request a Digital Certificate for the Domain.

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 Trust Anchor Root Certification Authorityissues 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 Private 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 Private 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 downloading, installing or otherwise taking delivery of a Digital Certificate constitutes acceptance of a Digital Certificate within the QuoVadis Private PKI.

4.4.3. Publication Of The Certificate By The Certification Authority

All Digital Certificates issued within the QuoVadis Private 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 Private 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 Private 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 Private PKI agrees to and accepts the Relying Party Agreement (http://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 or any other information in the Certificate.

The QuoVadis Private PKI does not support Certificate Renewal and the following do not apply to this CP/CPS:

- Circumstances for Certificate Renewal.
- Who may request certification of a new Public Key.
- Processing Certificate Renewal Requests.

- Notification of new Digital Certificate issuance to Certificate Holder.
- Conduct constituting acceptance of a Renewed Digital Certificate.
- Publication of the Renewed Digital Certificate by the Certification Authority.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

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 Private 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 Private PKI.

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

All Digital Certificate Re-Keys issued within the QuoVadis Private 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 Private 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). 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

In the event that an Issuing CA determines that its Digital Certificates or the QuoVadis Private 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 Private 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 Private PKI may revoke Digital Certificates that it has issued.
- A Registration Authority or Subscriber operating within the QuoVadis Private PKI may request revocation of Digital Certificates that it requested to be issued.
- Certificate Holders within the QuoVadis Private PKI may request revocation of their own Digital Certificates.
- An Application Software Vendor who has embedded a QuoVadis Trust Anchor Root Certification AuthorityCertificate 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 (http://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.

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

The Issuing CA must take commercially reasonable steps to revoke the Digital Certificate within 4 hours of receipt of a valid revocation request.

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

The Certificate Revocation List is published at least every twelve hours, and within 5-minutes of a Digital Certificate Revocation. The Certificate Revocation list is published and is available 24 hours a day, 7 days a week, and 52 weeks of the year every year.

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

The X.500 Directory provides Digital Certificate information services. QuoVadis seeks to provide availability for the X.500 Directory 7 days a week, 24 hours a day, subject to routine maintenance.

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.

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 Private PKI.

4.9.14. Who Can Request Suspension

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

4.9.15. Procedure For Suspension Request

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

4.9.16. Limits On Suspension Period

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

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

The Status of Digital Certificates issued within the QuoVadis Private 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.

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 Private 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 types of Digital Certificates under the QuoVadis Trust Anchor Root Certification Authority.

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 organization 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

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 Private 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 Private 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 organizations.

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 Private 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 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 to the highest industry standard.

5.3.4. Retraining Frequency And Requirements

QuoVadis provides and maintains a program of retraining in order to maintain appropriate and required levels of competency to perform job responsibilities to the highest industry standard.

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 roles of responsibility.

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

All events involved in the generation of the Certification Authority Key Pairs are recorded. This includes all configuration data used in the process.

Individuals who have access to particular Key Pairs and passwords will be audited. Key pair access will take the form of PIN-protected cryptographic smart cards. Access to the Oracle database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of two people must be present to perform certain tasks on the QuoVadis Certification Authority.

The types of data recorded by QuoVadis include but are not limited to;

- All data involved in each individual Digital Certificate registration process
- All data and procedures involved in the certification and distribution of Digital Certificates
- All data relevant to the publication of Digital Certificates and Certificate Revocation Lists
- All Digital Certificate revocation request details are recorded including reason for revocation
- Certificate and cryptographic hardware security lifecycle management is recorded
- External audit reports and QuoVadis Internal Audit reports
- Relevant application and system log files
- Physical access to QuoVadis data centres
- Security profile changes
- Activities of staff in PKI systems
- System failure, hardware failure and other anomalies

Audit logs will be appropriately time-stamped and their integrity protected.

5.4.2. Frequency Of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3. Retention Period For Audit Log

Audit logs relating to the certificate lifecycle are retained as archive records for a period no less than eleven (11) years for Swiss Qualified Certificates and for seven (7) years for all other Digital Certificates.

Detailed 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 Private 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 Private 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

Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the QuoVadis Private PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Issuing CA. Vulnerability assessment procedures intend to identify QuoVadis Private PKI threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders.

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 Private 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 Private 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 a CA Operations Disaster & Recovery Plan (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.
- 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 Private PKI;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained

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

All Key Pairs will be generated in a manner that QuoVadis, in its sole discretion, deems to be secure.

QuoVadis retains the right to generate the Certificate Holder's Private Key Pair. The Certificate Holder is required to provide all the necessary identification and authentication information when the Digital Certificate is being requested. Once all of the registration information is collected by the QuoVadis Certification Authority, the Certificate Holder's Key Pair are generated within a secure environment.

QuoVadis Certificate Holders can generate their own Private Key prior to submitting a Digital Certificate request. Key Generation methods and requirements differ according to the type of Digital Certificate requested.

Certificate Holder Key Generation may be performed in hardware or software depending on the Digital Certificate type.

All Keys for Issuing CAs, Registration Authorities and Registration Authority Officers must be randomly generated on an approved cryptographic token in a physically secure environment. CA Certificate signing keys are only used within this secure environment. Any pseudo random numbers used for Key generation material will be generated by a FIPS-approved method.

6.1.2. Private Key Delivery To Certificate Holder

In most cases, a Private Key will be generated and remain within the Cryptographic Module. If the owner of the Cryptographic Module generates the Key, then there is no need to deliver the Private Key. If a Key is not generated by the intended Key holder, then the person generating the Key in the Cryptographic Module (e.g., smart card) must securely deliver the Cryptographic Module to the intended Key holder. Accountability for the location and state of the Cryptographic Module must be maintained until delivery and possession occurs. The recipient will acknowledge receipt of the Cryptographic Module to the Issuing CA or Registration Authority. If the recipient generates the Key, and the Key will be stored by and used by the application that generated it, or on a Token in the possession of the recipient, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in PKCS#12) will be used. The resulting password-protected file may be kept on a magnetic medium or transported electronically.

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 Private PKI are determined by Certificate Profiles more fully disclosed in Appendix A. The QuoVadis Issuing CA uses an RSA minimum key length of 2,048-bit modulus. QuoVadis issuing CAs created after January 1, 2008 use an RSA minimum key length of 4,096-bit modulus.

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).

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

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 Private 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 Private 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. 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 Private 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.

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

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.

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

Private Keys held on a Cryptographic Module are stored in an encrypted form and password-protected.

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 Private PKI are validated to FIPS 140-2 Level-3 and/or EAL 4 security standards.

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 Private PKI are:

- Root CA Certificate 30 years

- All Issuing CA Certificates 10 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.

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

- Access controls to Certificate Authority services and PKI roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and PKI roles, see Section 5.2
- Identification and Authentication of personnel that fulfil roles of responsibility in the QuoVadis Private PKI, see Section 5.3
- Use of cryptography for session communication and database security, mutually authenticated and encrypted SSL/TLS is used for all communications
- Archival of Certificate Authority history and audit data, see Sections 5.4 and 5.6
- Use of x.509 Digital Certificates for all administrators.

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 Private 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 Private 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 Private 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
- 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.

7. CERTIFICATE, CRL, AND OCSP PROFILES

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 number assigned to each certificate	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.	Fixed
Certificate Policies	This extension contains Object Identifiers (OIDS) as well as a URL with a link to the QuoVadis Repository at http://www.quovadisglobal.com/repository. Certificates chaining up to the QuoVadis Trust Anchor Root Certification Authority do not have to contain OIDs in the Certificate Policies. However, such OIDs are useful to specify the QuoVadis Certificate Class. The following OIDs are relevant: 1.3.6.1.4.1.8024.0.4.2.0.1 - SSL Certificate Policy 1.3.6.1.4.1.8024.0.4.2.0.2 End User Certificate Policy	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.	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	Fixed

	The EKU in QuoVadis Digital Certificates is dependent on the QuoVadis Certificate Class and the Key Usage. Refer to Appendix A.	
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 3.1.1

7.1.5. Name Constraints

See 3.1.1

7.1.6. CP/CPS Object Identifier

The Object Identifiers (OIDs) assigned to this CP/CPS is 1.3.6.1.4.1.8024.0.4.

7.1.7. Usage Of Policy Constraints Extension

No Stipulation.

7.1.8. Policy Qualifiers Syntax And Semantics

Digital Certificates issued within the QuoVadis Private 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 Private 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 Private 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 Private PKI.

7.3.2. Online Certificate Status Protocol Extensions

No Stipulation.

7.4. LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL PROFILE

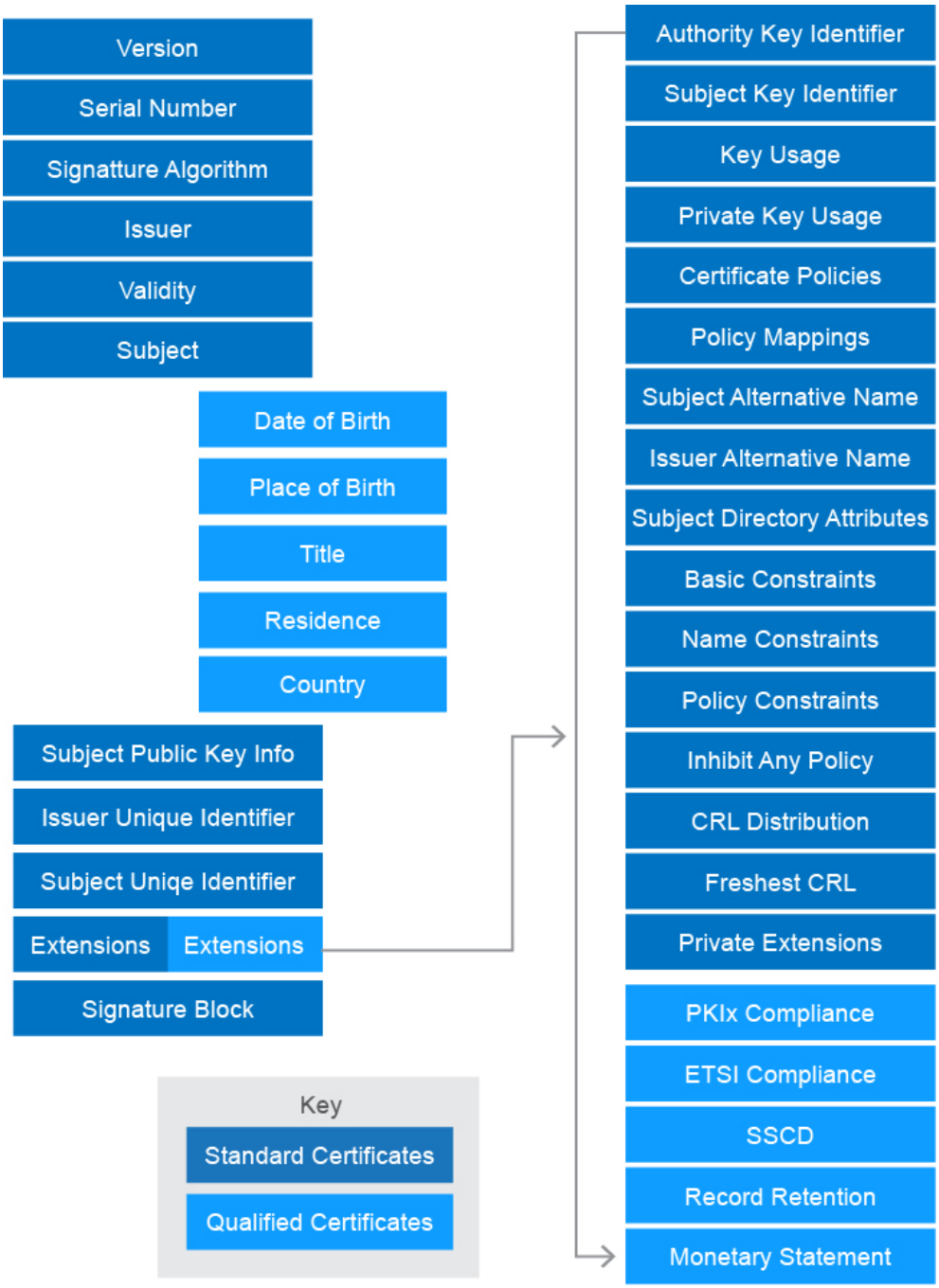
QuoVadis does not host a repository in the form of a Lightweight Directory Access Protocol directory for certificates issued by the QuoVadis Private PKI.

7.4.1. Lightweight Directory Access Protocol Version Numbers and Lightweight Directory Access Protocol Extensions

Not Applicable

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 http://www.quovadisglobal.com/repository.

7.5.2.1. QuoVadis Trust Anchor Root CA Certificate Hashes

Field	Certificate Profile
Serial Number	51be05846f1fb5c51c2f7274821ed1cdbc22a226
Signature Block	Key Id Hash(sha1): 1b c8 54 35 c6 3f 36 df 32 64 bd da e7 cd 60 73 d3 d9 e3 9e Key Id Hash(sha256): 7e0d1033f88569629c6837b071b421b1f76bb5d4c821248cc82a8a23dfcfcb15 Cert Hash(sha1): b7 15 9b 08 95 ec f2 a9 42 50 da 38 f3 3e 44 c0 a8 65 b9 c0 Cert Hash(sha256): e2f07045bf54350379acfe096e6e817e09718c5302eb0445d41e5a984a352479

7.5.2.2. QuoVadis Trust Anchor Root CA G2 Certificate Hashes

Field	Certificate Profile
Serial Number	1a5e4c5e6244ecafeacb0a25acc8eb3abff48d6c
Signature Block	Key Id Hash(sha1): 8c 1c f4 3b 19 9d 20 dc d5 83 75 2a 3e 77 d3 41 0a 73 81 f6 Key Id Hash(sha256): c253f40ec72eaf8835f108c09749d88204dda62ff96f5988ff95656e41b6a3dd Cert Hash(sha1): 5c f4 a2 58 0f f6 e0 73 98 6f a1 09 cd 47 06 8d d6 9f 77 73 Cert Hash(sha256): a77b973bff1bf6f81353d22b906fd31e5e081a5478fc3c30fc96cc57863db777

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY, CIRCUMSTANCE AND STANDARDS OF ASSESSMENT

8.1.1. QuoVadis Certification Authority

The QuoVadis Private PKI is not subject to the audit assessments that apply to the publicly trusted PKI.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

Issuing CAs and Registration Authorities within the QuoVadis Private PKI will make available all applicable fees upon request. Fees for Digital Certificate issuance vary widely based upon volumes and Digital Certificate types.

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 excess of the of CHF 2 (Two) Million per occurrence and CHF 8 (Eight) Million annual aggregate.

Within the QuoVadis Private 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 Private 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 Private 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 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 Private 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 Private 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 Private 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;

- the termination of a Issuing CA within the QuoVadis Private 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 Trust Anchor 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 Private 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

9.6.1.1. Root Certification Authority Representations

QuoVadis discharges its obligations by:

- providing the operational infrastructure and certification services, including X.500 Directory and service provider software;
- making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” include but do not limit QuoVadis to operating in compliance with:
  - documented operational procedures; and
  - within applicable law and regulation;
- approving the establishment of all Issuing CAs and on approval, executing an Issuing CA Agreement (save in respect of the QuoVadis Issuing CA);
- maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation;

- publishing its QuoVadis CA Certificates at http://www.quovadisglobal.com/repository and other nominated web sites;
- issuing CA Certificates to Issuing CAs that comply with X.509 standards and are suitable for the purpose required;
- issuing CA Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
- publishing issued Issuing CA Certificates without alteration in the X.500 Directory;
- investigating any suspected compromise which may threaten the integrity of the QuoVadis Private PKI;
- revoking Issuing CA Certificates and posting such revoked Certificates in the X.500 Directory Certificate Revocation List; and
- conducting compliance audits of Issuing CAs.

9.6.1.2. Issuing Certification Authority Warranties

An Issuing CA hereby warrants that Digital Certificates shall be revoked if the Issuing CA believes or is 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.

The Issuing CA 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.

Each Issuing CA is required to ensure that warranties, if any, provided by QuoVadis in connection with this QuoVadis CP/CPS to Certificate Holders and Authorised Relying Parties are incorporated, by reference or otherwise, in the relevant Certificate Holder Agreement or applicable terms and conditions. Other warranties, if any, provided to Certificate Holders and/or Authorised Relying Parties shall be set out in a warranty protection plan duly approved by the Policy Management Authority and adopted by QuoVadis.

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 Private 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

Certificate Holders represent and warrant that:

- The Private Key is protected and has never been accessed by another person.

- All representations made by the Certificate Holder in the Digital Certificate Application are true.
- All information in the Digital Certificate is true and accurate.
- The Digital Certificate is being used for its intended, authorised and legal purpose consistent with this CP/CPS.
- They will promptly request revocation of the Digital 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 Private Key associated with the Public Key listed in the Digital Certificate.

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 Private 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 Private 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).

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 Private PKI (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the QuoVadis Private 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 Private 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
QV Trust Anchor Device	US $2500

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

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 Private PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the QuoVadis Private 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 Private 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 http://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

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

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.

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 Private PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. All Digital Certificate Profiles within the QuoVadis Private 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 Certificate Class OID
QV Trust Anchor Device	Issued to devices, including SSL Certificates. Includes Domain Controller certificates and Gateway certificates.	1.3.6.1.4.1.8024.0.4.2.0.1
QV Trust Anchor End User	Issued to natural persons.	1.3.6.1.4.1.8024.0.4.2.0.2

10.2. QV TRUST ANCHOR END USER

PURPOSE		
QV Trust Anchor End User Digital Certificates provide flexibility for a range of uses appropriate to their reliance value including electronic signatures, authentication, and encryption. There are no specified Identification and authentication procedures for issuance of certificates under the QVTARCA, except that Certificates may not be issued with contents which are misleading, attempt to convey authority which does not exist or breach the intellectual property rights of an individual or entity whether registered or not.		
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
Organisational Unit (OU)	Variable Data	Holder Variable
Organisation (O)	Organisation legal name	Holder Variable
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 Trust Anchor End User Certificate Class OID = 1.3.6.1.4.1.8024.0.4.2.0.2.	Fixed

10.3. QV TRUST ANCHOR DEVICE

PURPOSE		
QuoVadis Device Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols There are no specified Identification and authentication procedures for issuance of certificates under the QVTARCA, except that Certificates may not be issued with contents which are misleading, attempt to convey authority which does not exist or breach the intellectual property rights of an individual or entity whether registered or not. 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.		
Fields	**Content**	**Demarcation**
Subject		
Common Name (CN)	Subject Common Name	Holder Variable
Organisational Unit (OU)	Variable Data	Holder Variable
Organisation (O)	Organisation legal name	Holder Variable
Locality (L)	Subject Locality	Holder Variable
State/Province (ST)	Subject State/Province	Holder Variable
Country (C)	Subject 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) Secure Email (1.3.6.1.5.5.7.3.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) 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 should 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 Trust Anchor Device Certificate Class OID = 1.3.6.1.4.1.8024.0.4.2.0.1.	Fixed

11. APPENDIX B

11.1. 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 Private PKI unless context otherwise requires:

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

"Application Software Vendors" 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 KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, Red Hat Inc., Adobe, 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.

"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).

"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 Private 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 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 Private PKI.

"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 Private 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 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.

"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 Private 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; (v) 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.

"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 Private PKI.

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

"Issuing CA Certificate" A Digital Certificate issued by the QuoVadis Trust Anchor Root Certification Authorityto 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 Private 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 Private 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 the European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

"QuoVadis" means QuoVadis Limited, a Bermuda exempted company.

"QuoVadis Issuing Certification Authority" means QuoVadis in its capacity as an Issuing CA.

"QuoVadis Private 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.

"Registration Authority" means a Registration Authority designated by an Issuing CA to operate within the QuoVadis Private 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 Private 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 Private PKI.

"Registration Authority Officer" means an Individual designated by a Registration Authority as being authorised to perform the functions of that Registration Authority.

"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.

"Reserved IP Address" means an IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

"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 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.

"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).

"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 Private 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).