



**QUOVADIS ROOT CERTIFICATION AUTHORITY  
CERTIFICATE POLICY/  
CERTIFICATION PRACTICE STATEMENT**

**OIDs:**                    **1.3.6.1.4.1.8024.0.1**  
                              **1.3.6.1.4.1.8024.0.3**

**Effective Date:**   **29 October 2007**

**Version:**               **4.4**

## Important Note About this Document

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

This document covers aspects of the QuoVadis PKI that relate to all CAs established by QuoVadis under the QuoVadis Root Certification Authority and the QuoVadis Root Certification Authority 3 (QuoVadis Root CA 3). There are a number of instances where the legal and regulatory framework regarding the issuance of Qualified Certificates under either the Swiss or European Digital Signature regimes require deviation from QuoVadis standard practices. In these instances, this Document shows these differences either by indicating in the body of the text "For Qualified Certificates" or with the inclusion of a Text Box as follows:

This is a provision specifically about Qualified Certificates.

## 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.quovadis.bm](http://www.quovadis.bm)  
 Electronic mail: [policy@quovadis.bm](mailto:policy@quovadis.bm)

## Version Control:

<b>Author</b>	<b>Date</b>	<b>Version</b>	<b>Comment</b>
QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	WebTrust Revisions
QuoVadis PMA	01 April 2004	2.07	WebTrust Revisions
QuoVadis PMA	11 November 2005	2.08	WebTrust Revisions
QuoVadis PMA	17 April 2006	4.00	Cumulative ZertES Revisions
QuoVadis PMA	14 September 2006	4.1	EIDI-V Certificate Requirements
QuoVadis PMA	26 February 2007	4.2	QuoVadis Root CA 3 Added
QuoVadis PMA	03 April 2007	4.3	Clarifications to Appendix A
QuoVadis PMA	29 October 2007	4.4	General Edits and RFC3647 Conformity, Cumulative ZertES and EIDI-V Revisions

**Table of Contents**

**1. INTRODUCTION ..... 1**

1.1. Overview .....1

1.2. Document Name, Identification and Applicability .....2

1.3. Public Key Infrastructure Participants.....2

1.4. Certificate Usage .....7

1.5. Policy Administration.....8

1.6. Definitions and Acronyms.....8

**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 .....9

3.2. Initial Identity Validation .....10

3.3. Identification And Authentication For Renewal Requests .....12

3.4. Identification and Authentication For Revocation Requests.....12

**4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS ..... 12**

4.1. Certificate Application .....12

4.2. Certificate Application Processing.....13

4.3. Certificate Issuance .....13

4.4. Certificate Acceptance.....14

4.5. Key Pair And Certificate Usage .....15

4.6. Certificate Renewal.....15

4.7. Certificate Re-Key.....15

4.8. Certificate Modification.....16

4.9. Certificate Revocation And Suspension.....16

4.10. Certificate Status Services .....19

4.11. End Of Subscription .....19

4.12. Key Archival And Recovery.....19

**5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ..... 19**

5.1. Physical Controls .....19

5.2. Procedural Controls .....20

5.3. Personnel Controls.....21

5.4. Audit Logging Procedures.....22

5.5. Records Archival.....23

5.6. Key Changeover .....24

5.7. Compromise And Disaster Recovery.....24

5.8. Certification Authority And/Or Registration Authority Termination .....25

**6. TECHNICAL SECURITY CONTROLS ..... 25**

6.1. Key Pair Generation And Installation.....25

6.2. Private Key Protection And Cryptographic Module Engineering Controls .....26

6.3. Other Aspects Of Key Pair Management .....28

6.4. Activation Data .....28

6.5. Computer Security Controls .....29

6.6. Life Cycle Technical Controls .....29

6.7. Network Security Controls .....30

6.8. Time-Stamping.....30

**7. CERTIFICATE, CRL, AND OCSP PROFILES ..... 30**

7.1. Certificate Profile .....30

7.2. Certificate Revocation List Profile .....31

7.3. Online Certificate Status Protocol Profile .....31

7.4. Lightweight Directory Access Protocol Profile.....31

7.5. Root And Issuing Certification Authority Profiles And Certificate Fields .....32

**8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS ..... 41**

8.1. Frequency, Circumstance And Standards Of Assessment .....41

8.2. Identity And Qualifications Of Assessor .....41

---

8.3.	Assessor's Relationship To Assessed Entity.....	42
8.4.	Topics Covered By Assessment.....	42
8.5.	Actions Taken As A Result Of Deficiency .....	42
8.6.	Publication Of Audit Results.....	43
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS.....</b>	<b>43</b>
9.1.	Fees .....	43
9.2.	Financial Responsibilities .....	43
9.3.	Confidentiality Of Business Information.....	44
9.4.	Privacy Of Personal Information .....	44
9.5.	Intellectual Property Rights .....	46
9.6.	Representations And Warranties.....	46
9.7.	Disclaimers Of Warranties .....	48
9.8.	Liability and Limitations of Liability.....	48
9.9.	Indemnities.....	50
9.10.	Term And Termination .....	50
9.11.	Individual Notices And Communications With Participants .....	50
9.12.	Amendments.....	50
9.13.	Dispute Resolution Provisions.....	51
9.14.	Governing Law .....	51
9.15.	Compliance With Applicable Law.....	52
9.16.	Miscellaneous Provisions .....	52
9.17.	Other Provisions .....	52
<b>10.</b>	<b>APPENDIX A .....</b>	<b>53</b>
10.1.	Digital Certificate Profiles .....	53
10.1.1.	Standard Test Certificate.....	54
10.1.2.	Standard Personal Certificate .....	56
10.1.3.	Qualified Certificate .....	58
10.1.4.	Standard Commercial Certificate.....	60
10.1.5.	Commercial - EIDI-V Certificates .....	62
10.1.6.	Special Purpose Certificates.....	64
10.1.7.	Closed Community Certificates .....	66
<b>11</b>	<b>APPENDIX B .....</b>	<b>67</b>
11.1	Definitions and Acronyms.....	67

## 1. INTRODUCTION

### 1.1. Overview

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

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

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

In the provision of Trust Services, QuoVadis maintains several accreditations and certifications of its Public Key Infrastructure. These include:

- 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.
- 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) entitled to issue and administer qualified electronic certificates, conducted by KPMG. 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.

QuoVadis ensures the integrity of its PKI operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between QuoVadis and any Participant in the QuoVadis PKI. This CP/CPS merely provides a general overview of the QuoVadis PKI including Digital Certificate Profiles as defined in Appendix A.

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

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 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 Identifier assigned for the certificate policy extension for certificates issued under the QuoVadis Root Certification Authority Certificate is 1.3.6.1.4.1.8024.0.1, while the OID assigned by QuoVadis for certificates issued under the QuoVadis Root CA 3 Certificate is 1.3.6.1.4.1.8024.0.3. These are used as the OID arcs for QuoVadis to identify the Certificate Policies under which it issues certificates pursuant to this CP/CPS:

QuoVadis Root Certification Authority	1.3.6.1.4.1.8024.0.1
QuoVadis Root CA 3	1.3.6.1.4.1.8024.0.3

The certificate policy extension in certificates issued in accordance with this CP/CPS shall assert at least one of these OID arcs. The QuoVadis Root Certification Authority has cross-certified the QuoVadis Root CA 2. QuoVadis Root CA 2 is used to issue Extended Validation (EV) SSL Certificates associated with EV OID 1.3.6.1.4.1.8024.0.2.100.1.2, and Digital Certificates issued under Root CA 2 have their own CP/CPS.

This QuoVadis CP/CPS is applicable to all Digital Certificates issued by the QuoVadis Root Certification Authority and by Issuing CAs. Digital Certificates issued under this CP/CPS are intended to support secure electronic commerce and the secure exchange of information by electronic means.

## 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:

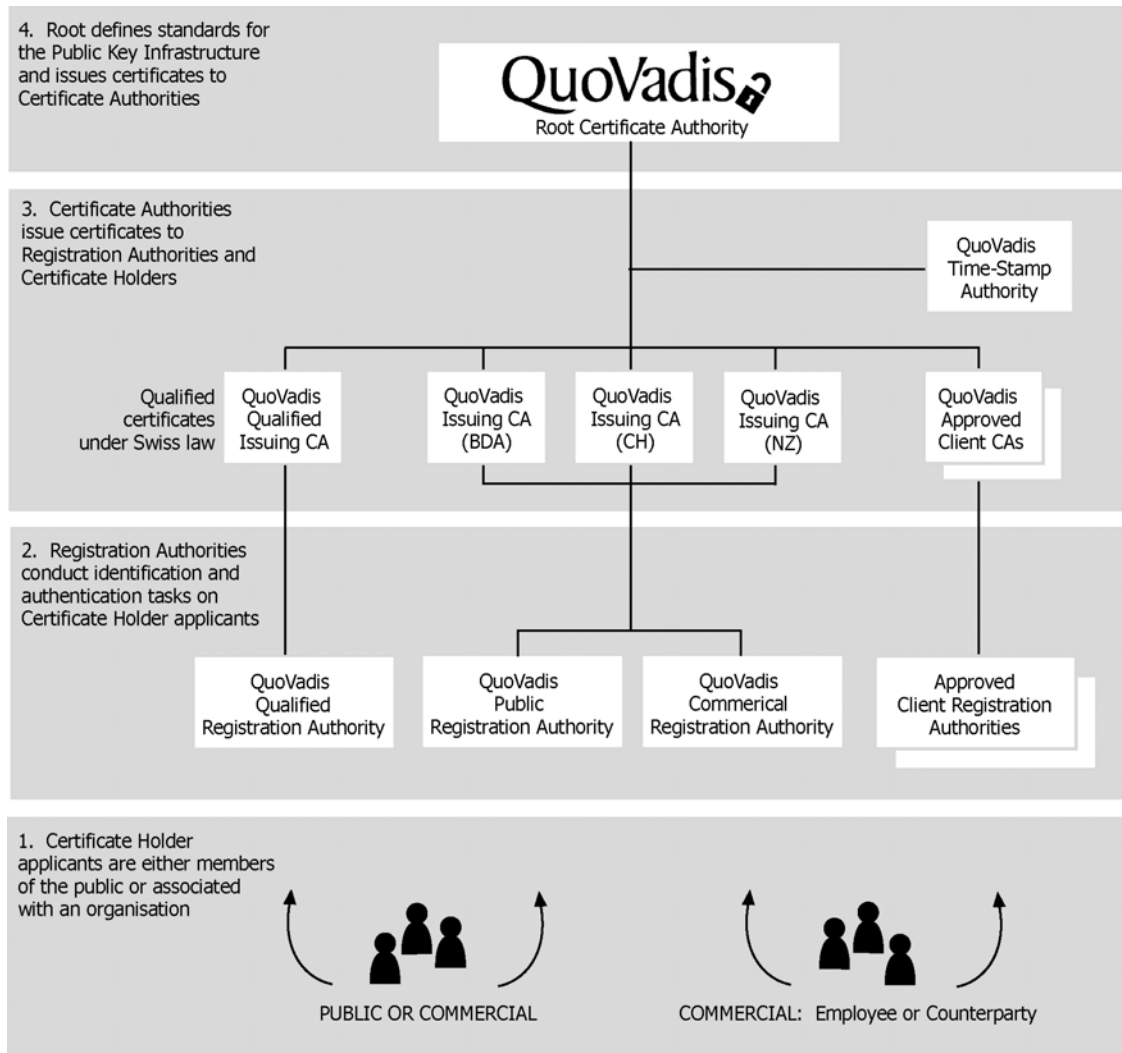
- Issuing Certification Authority services.
- Registration Authority services.

QuoVadis, in its capacity as the Root Certification Authority, holds the QuoVadis Root Certificates. The QuoVadis Root Certification Authority represents the apex of the QuoVadis PKI. The QuoVadis Root Certification Authority digitally creates, signs and issues Issuing Certification Authority Certificates using one of the Root Certificates identified above. Issuing CA Certificates are only issued to Approved Issuing Certification Authorities. An Approved Issuing CA utilises its Issuing CA Certificate to create, sign and issue Digital Certificates. Approved Registration Authorities act as the interface between Issuing CAs and an Applicant for a Digital Certificate. Approved Registration Authorities perform due diligence on potential Digital Certificate Holders and only successful applicants are approved and receive Digital Certificates.

An Authorised Issuing CA may also issue Device Certificates to itself, Subsidiaries or Holding Companies to Identify and Authenticate its Devices. Approved Registration Authorities perform due diligence on potential Device Certificate Holders and only successful Device Certificate applicants are approved and receive Device 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.

The diagram below illustrates the components of the QuoVadis PKI:



QuoVadis provides identification and authentication services for Digital 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.

For Qualified Digital Certificates according to the Swiss Digital Signature Law, all identification processes for individuals require applicants to present themselves for face-to-face verification.

QuoVadis has established the QuoVadis Root Certification Authority under which a number of subordinate services operate. These subordinate services within the QuoVadis PKI are either:

- managed and operated by QuoVadis; or
- managed by clients but operated by QuoVadis (outsourced services); or
- managed and operated by clients (external services).

This CP/CPS describes all subordinate services that operate under the QuoVadis Root Certification Authority, i.e. that are within the QuoVadis “chain of trust”.

Participants (“Participants”) within the QuoVadis PKI include:

- Certification Authorities

- Registration Authorities
- Digital Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance
- 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 primary purpose of the CP/CPS, of describing the uniformity and efficiency of practices throughout the QuoVadis PKI.

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

- are the minimum requirements necessary to ensure that Digital 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 the latest in Internet Standards (x509 v.3) as set out in 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.

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

### **1.3.1. Certification Authorities**

#### **1.3.1.1 Root Certification Authority**

The QuoVadis PKI contains several Root Certificates, each with a distinct common name for its Issuer and Subject. One QuoVadis Root Certification Authority is named "QuoVadis Root Certification Authority" and another has a common name for its Issuer and Subject of "QuoVadis Root CA 3." Under both Root Certificates, the QuoVadis Certification Authority issues Issuing CA Certificates and Time Stamping Authority Certificates in accordance with this QuoVadis CP/CPS and related operational documents.

#### **1.3.1.2 QuoVadis Obligations**

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

#### **1.3.1.3 Issuing Certification Authorities**

In addition to the QuoVadis Issuing CAs, other Issuing CAs are Organisations that have been authorised by QuoVadis to participate within the QuoVadis PKI to issue, revoke and otherwise manage Digital Certificates in accordance with their respective Issuing Certification Authority Agreements and this CP/CPS. Generally, Issuing CAs will be authorised to issue and manage all types of Digital Certificates supported by this CP/CPS.

In accordance with the Swiss Digital Signature law, Qualified Certificates will only be issued from Issuing Certification Authorities owned and operated by QuoVadis.

An Organisation wishing to participate in the QuoVadis PKI, in the capacity of an 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 Issuing CAs will be required to enter into and act in accordance with an Issuing Certification Authority Agreement and this CP/CPS. Without limitation to the generality of the foregoing, Issuing CAs are required to act in accordance with and to be bound by the terms of 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. QuoVadis operates the QuoVadis Root Certification Authority and QuoVadis Issuing Certification Authorities in accordance with this CP/CPS. Notwithstanding that an Issuing CA may delegate certain functions to a Registration Authority; the Issuing CA shall retain all responsibility for the management of Digital Certificates issued by it.

#### **1.3.1.4 Issuing CA Obligations**

Within the QuoVadis PKI all Issuing CAs are responsible for the management of Digital Certificates issued by them. Digital Certificate Management includes all aspects associated with the application, issue and revocation of Digital Certificates, including any required identification and authentication processes included in the Digital Certificate application process. Issuing CAs, if authorised to do so by QuoVadis, may rely on third party Registration Authorities in the performance of Digital 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 Digital Certificate Holders.

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

Without limitation to the generality of the foregoing, Issuing CAs are required to ensure that;

- Their 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, and 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 Certification Authority Agreement.

#### **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 Registration Authorities 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 Registration Authority and the relevant Issuing CA.

QuoVadis Registration Authorities 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**

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

- 
- Both as an applicant for a Digital Certificate and as a Digital Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate.
  - 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.
  - Take all reasonable measures to avoid the compromise of the security or integrity of the QuoVadis PKI.
  - Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
  - At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.
  - Use the signing key pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Digital Certificate Holder.
  - Discontinue the use of the digital signature key pair in the event that QuoVadis notifies the Digital Certificate Holder that the QuoVadis PKI has been compromised.

#### **1.3.3.2. Accepted Limitation Of Liability**

Digital Certificates include a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this CP/CPS. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

#### **1.3.4. Relying Parties**

Authorised Relying Parties are Individuals or Organisations who are authorised by contract to exercise Reasonable Reliance on Digital Certificates in accordance with the terms and conditions of this CP/CPS.

##### **1.3.4.1. Obligations and Responsibilities**

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

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

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

##### **1.3.4.2. Reasonable Reliance**

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

- that the attributes of the Digital Certificate relied upon are appropriate in all respects to the reliance placed upon that Digital Certificate by the Authorised Relying Party including, without limitation to the generality of the foregoing, the level of Identification and Authentication required in connection with the issue of the Digital Certificate relied upon.
- that the Authorised Relying Party has, at the time of that reliance, used the Digital Certificate for purposes appropriate and permitted under this QuoVadis CP/CPS ;
- that the Authorised Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Authorised Relying Party;

- that the Digital Certificate intended to be relied upon is valid and has not been revoked, the Authorised Relying Party being obliged to check the status of that Digital Certificate utilising either the QuoVadis Database, the QuoVadis Certificate Revocation List, or the QuoVadis Online Certificate Status Protocol and otherwise in accordance with the provisions of this QuoVadis CP/CPS ;
- that the Authorised Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- that the Authorised Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Digital Certificate being relied upon.
- that the Authorised Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
- that the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
- that the identity of the Digital 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 brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this CP/CPS. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers.

#### **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 for certificate revocation.

#### **1.3.5. Other Participants**

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant QuoVadis documentation.

### **1.4. Certificate Usage**

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

#### **1.4.1. Appropriate Certificate Usage**

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

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

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

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

**1.4.2. Prohibited Certificate Usage**

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

According to Swiss Digital Signature law (ZertES), TAV SR 943.032.1 and ETSI TS 101 456 the only appropriate use for Qualified Digital Certificates is signing.

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

**1.5. Policy Administration****1.5.1. Organisation Administering the CP/CPS**

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

**1.5.2. Contact Person**

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

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

Website: [www.quovadis.bm](http://www.quovadis.bm)  
Electronic mail: [policy@quovadis.bm](mailto:policy@quovadis.bm)

**1.5.3. Person Determining the CP/CPS Suitability**

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

**1.5.4. CP/CPS Approval Procedures**

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

**1.5.4.1. Publication of CP/CPS**

This CP/CPS is published electronically in PDF format at [www.quovadis.bm](http://www.quovadis.bm).

**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 does operate access controls in connection with the availability of documentation. Access is generally available only to participants in the QuoVadis PKI where deemed necessary.

**1.6. Definitions and Acronyms**

See Appendix B.

---

## **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

### **2.1. Repositories**

The QuoVadis Repository serves as the primary repository. However, copies of the X.500 Directory may be published at such other locations as are required for the efficient operation of the QuoVadis PKI.

### **2.2. Publication of Certificate Information**

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

### **2.3. Time or Frequency of Publication**

Digital Certificate information is published promptly following generation and issue and within 20 minutes of being revoked.

### **2.4. Access Controls on Repositories**

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

## **3. IDENTIFICATION AND AUTHENTICATION**

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

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

### **3.1. Naming**

#### **3.1.1. Types Of Names**

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

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

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

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

Alternatively, Distinguished Names may be based on domain name components, e.g. CN=John Smith, DC=QuoVadis, DC=BM.

The Common Name may contain the applicant's first and last name (surname). The Common Name, the Organisation (O) or Domain Name (DC), and the Organisational Unit (where applicable), are the only fields authenticated during the Registration procedure. The User may choose whether to include the Locality, State and Country, but they are not verified in any way. Such attributes do not necessarily indicate the Certificate Holder's country of citizenship, country of residence, or the country of issuance of the Digital Certificate.

For Qualified Certificates issued according to the Swiss Digital Signature law, all fields containing information must be verified by the appropriate Registration Authority by reference to appropriate documentation and face-to-face presentation of Government-Issued ID or Passport.

### **3.1.2. Need For Names To Be Meaningful**

Distinguished Names must be meaningful, unambiguous and unique. Pseudonymous names may be used. QuoVadis supports the use of Digital Certificates as a form of identification within a particular community of interest.

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

### **3.1.3. Pseudonymous Certificate Holders**

QuoVadis Registration Authorities, their Subsidiaries or Holding Companies may request Class 5 (Pseudonym) Digital Certificates to be issued by the QuoVadis Issuing CA to Employees of the Nominating Registration Authority, their Subsidiaries or Holding Companies.

### **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 Digital Certificate subject's 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.

For Qualified Certificates, in accordance with Swiss Digital Signature law, private keys are generated on secure signature smartcards in the presence of the Certificate Holder. The Certificate Holder is responsible for securing the smartcard with a Personal Identification Number directly on the Secure Signature Creation Device (SSCD).

### 3.2.2. Authentication Of Organisation Identity

The Identity of an Organisation is required to be Authenticated with respect to each Digital Certificate that asserts (i) the Identity of an Organisation; or (ii) an Individual or Device's affiliation with an Organisation. Without limitation to the generality of the foregoing, the Identity of any Organisation that seeks to act as a Registration Authority for its employees and/or employees of its respective Subsidiaries, Holding Companies or Counterparties is required to be Authenticated.

In order to Authenticate the Identity of an Organisation, at a minimum, confirmation is required that: (i) the Organisation legally exists in the name that will appear in the Distinguished Name of any Digital Certificates issued under its name, or is legally recognised as doing business under an alternative proposed by the Organisation; and (ii) all other information contained in the Digital Certificate application is correct.

Registration information provided by an Organisation may be validated by reference to official government records and/or information provided by a reputable vendor of corporate information services. The accuracy and currency of such information may be validated by conducting checks with financial institution references, credit reporting agencies, trade associations, and other entities that have continuous and ongoing relationships with the Organisation under review. In addition, the telephone number provided by the Organisation as the telephone number of its principal place of business may be called to ensure that the number is active and answered by the Organisation.

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

For Qualified Certificates, in accordance with Swiss Digital Signature law, certificates are only issued to natural persons. These persons may have an affiliation to an organisation which is verified by appropriate documentation.

### 3.2.3. Authentication Of Individual Identity

An Individual's Identity is to be authenticated in accordance with all relevant application data and other documentation.

### 3.2.4. Non-Verified Certificate Holder Information

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

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

- Email address
- Organisational Unit
- Locality

For Qualified Certificates, in accordance with the Swiss Digital Signature law, all certificate fields and registration information are verified by appropriate documentation.

### 3.2.5. Validation Of Authority

Where an Applicant's Name is to be associated with an Organisational Name to indicate his or her status as a Counterparty, Employee or specifies an Authorisation level to act on behalf of an Organisation, the Registration Authority will validate the Applicant's Authority by reference to business records maintained by the Registration Authority, its Subsidiaries, Holding Companies or Affiliates.

### **3.2.6. Criteria For Interoperation**

The QuoVadis PKI operates in accordance with open standards under the x.509 criteria and as such Digital Certificates issued by the QuoVadis Issuing CA are fully interoperable with Digital Certificates issued by other Issuing CAs. The QuoVadis Root Certification Authority private key is used to cross-certify QuoVadis Root CA 2 and QuoVadis Root CA 3. The QuoVadis Root Certification Authority private key and the QuoVadis Root CA 3 Private Keys are used to sign the public keys of subordinate Issuing CAs, which may be enterprise CAs operated by QuoVadis' customers. Otherwise, QuoVadis CAs and subordinate CAs are not cross-certified with any other Certification Authority.

### **3.3. Identification And Authentication For Renewal Requests**

QuoVadis does not support renewal. Key Pairs must always expire at the same time as the associated Digital Certificate. If a renewal request is accepted, both new Digital Certificates and new Key Pairs are issued. Renewal is not permitted after Digital Certificate revocation. Application for a Digital Certificate following revocation is treated as though the person requesting renewal were a new Applicant.

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

Identification and Authentication for routine re-key is based on the same requirements as issuance of new certificates.

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

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

### **3.4. Identification and Authentication For Revocation Requests**

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

#### **3.4.1. Issuing Certification Authority**

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

#### **3.4.2. Registration Authority**

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

#### **3.4.3. Certificate Holder**

A Digital 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;

For Qualified Certificates, in accordance with the Swiss Digital Signature law, proof of identification can only take the form of a Passport or Government-issued ID Card.

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

Each Issuing CA may adopt its own application forms and procedures, which Applicants will be required to satisfy. Each Holder of a Digital Certificate is required to be bound by contract with respect to the use of that Digital Certificate. These contracts may be directly between the Issuing CA and the Holder or imposed upon that Holder through terms and conditions binding upon him or her. All agreements concerning the use of, or reliance upon, Digital Certificates issued within the QuoVadis PKI must incorporate by reference the requirements of this QuoVadis CP/CPS as it may be amended from time to time.

### **4.2. Certificate Application Processing**

#### **4.2.1. Performing Identification And Authentication Functions**

See Appendix A 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 Digital Certificate Holder applications based upon the Digital 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 Digital Certificate Holder Application.

#### **4.2.3. Time To Process Certificate Applications**

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

### **4.3. 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 Certification Authority Agreement by the Issuing CA, successful completion of the Issuing Certification Authority application process as prescribed by QuoVadis, and final approval of the application by the QuoVadis Root Certification Authority, the QuoVadis Root Certification Authority issues the Issuing Certification Authority 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 by the nominating Issuing CA, the Registration Authority becomes duly appointed, and appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

##### **4.3.1.4. Registration Authority Officer's Certificate**

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

#### 4.3.1.5. Certificate Holder Certificates

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

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

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

#### 4.4. Certificate Acceptance

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

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

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

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

##### 4.4.1. Notice Of Acceptance

BY ACCEPTING A DIGITAL CERTIFICATE, THE CERTIFICATE HOLDER ACKNOWLEDGES THAT HE OR SHE AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CERTIFICATE POLICY & CERTIFICATION PRACTICE STATEMENT AND THE APPLICABLE CERTIFICATE HOLDER AGREEMENT. ALSO BY ACCEPTING A DIGITAL CERTIFICATE, THE DIGITAL 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.

BY ACCEPTING A DIGITAL CERTIFICATE, THE CERTIFICATE HOLDER ALSO AGREES TO INDEMNIFY AND HOLD QUOVADIS AND ITS AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS, PROCEEDINGS, OR CLAIMS, AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS FEES, THAT QUOVADIS, ITS AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A DIGITAL CERTIFICATE AND THAT ARISE FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE CERTIFICATE HOLDER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE CERTIFICATE HOLDER); (II) FAILURE BY THE CERTIFICATE HOLDER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE QUOVADIS OR ANY PERSON RECEIVING OR RELYING ON THE DIGITAL CERTIFICATE; (III) FAILURE TO PROTECT THE PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORISED USE OF THE DIGITAL CERTIFICATE HOLDER'S PRIVATE KEY; (IV) USE OF THE

---

DIGITAL CERTIFICATE FOR A PURPOSE WHICH IS LIBELLOUS OR CONSTITUTES MALICIOUS FALSEHOOD OR DISPARAGEMENT OF GOODS OR SERVICES, OR IS OTHERWISE DEFAMATORY, IS IMMORAL, OBSCENE, PORNOGRAPHIC, IS ILLEGAL OR ADVOCATES ILLEGAL ACTIVITY, OR CONSTITUTES A VIOLATION OF PRIVACY OR INFRINGES ON THE INTELLECTUAL PROPERTY RIGHTS OF QUOVADIS OR A THIRD PARTY.

#### **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 PKI.

#### **4.4.3. Publication Of The Certificate By The Certification Authority**

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

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

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

### **4.5. Key Pair And Certificate Usage**

#### **4.5.1. Certificate Holder Private Key And Certificate Usage**

Within the QuoVadis PKI, a Certificate Holder may only use the Private Key and corresponding Public Key in the Digital Certificate for their lawful and intended use. The Digital 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**

A Party seeking to rely on a Digital Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement ([www.quovadis.bm/policies](http://www.quovadis.bm/policies)) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

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

- Circumstances for Digital Certificate Renewal.
- Who may request certification of a new public key.
- Processing Digital Certificate Renewal Requests.
- Notification of new Digital Certificate issuance to subscriber.
- 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**

On expiration of the Certificate Validity Period, Digital Certificates are renewed on the basis of issuing a new Key Pair to the Digital Certificate Holder. 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 renewed 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 Digital 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 the Digital Certificate to be renewed, the Certificate Holder may digitally sign an electronic message to the Nominating Registration Authority requesting that the Digital Certificate be renewed and confirming that the original application details have not changed.

**4.7.4. Notification Of New Certificate Issuance To Certificate Holder**

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

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

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

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

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

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

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

**4.8. Certificate Modification**

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

- Circumstance for Digital Certificate modification.
- Who may request Digital Certificate modification.
- Processing Digital Certificate modification requests.
- Notification of new Digital Certificates issuance to subscriber.
- Conduct constituting acceptance of modified Digital Certificate.
- Publication of the modified Digital Certificate.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

**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
- Digital 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 Digital 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;
- Where a Digital 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 Digital Certificate Holder
  - The Digital Certificate Holder is no longer authorised to act on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
  - The Digital 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
- Digital Certificate Holder bankruptcy
- Digital Certificate Holder liquidation
- Digital Certificate Holder death
- Digital 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 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:

##### **4.9.2.1. QuoVadis**

QuoVadis may revoke any Digital Certificate issued within the QuoVadis PKI at its sole discretion, and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.

##### **4.9.2.2. Issuing Certification Authorities**

An Issuing CA operating within the QuoVadis PKI may revoke Digital Certificates that it has issued.

##### **4.9.2.3. Registration Authorities**

A Registration Authority operating within the QuoVadis PKI may request revocation of Digital Certificates that it requested to be issued.

##### **4.9.2.4. Certificate Holder**

Digital Certificate Holders within the QuoVadis PKI may request revocation of their own Digital Certificates.

#### **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 Digital Certificate Holder may be required to submit the revocation request via the QuoVadis Support Line or directly over an Internet connection. The Digital 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.

#### **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 revoke the Digital Certificate within 2 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 5-minute intervals, 24 hours a day, 7 days a week, and 52 weeks of the year every year. The Certificate Revocation List in the X.500 Directory is updated at the time of Digital Certificate Revocation.

When an Issuing CA provides Certificate Revocation Lists as a method of verifying the validity and status of Digital Certificates, the following requirements will apply:

- Authorised Relying Parties who rely on a Certificate Revocation List must in their validation requests check a current, valid Certificate Revocation List for the Issuing CA in the Digital Certificate path and obtain a current Certificate Revocation List; and
- Authorised Relying Parties who rely on a Certificate Revocation List must (i) check for an interim Certificate Revocation List before relying on a Digital Certificate, and (ii) log their validation/revocation checks.

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

**4.9.8. 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**

When an Issuing CA provides an online Digital Certificate status database as a method of verifying the validity and status of Digital Certificates, the Authorised Relying Party must validate the Digital Certificate in accordance with that method and log the validation request and response.

An entity that downloads a Certificate Revocation List from a repository shall verify the authenticity of the Certificate Revocation List by checking its digital signature and the associated Digital Certificate path.

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**

There are no other forms of Revocation Advertisements available.

**4.9.12. Special Requirements Re-Key Compromise**

QuoVadis does not support re-key.

**4.9.13. Circumstances For Suspension**

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

**4.9.14. Who Can Request Suspension**

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

**4.9.15. Procedure For Suspension Request**

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

**4.9.16. Limits On Suspension Period**

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

#### **4.10. Certificate Status Services**

##### **4.10.1. Operational Characteristics**

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List [www.quovadisoffshore.com/crl/issuing\\_ca\\_name.crl](http://www.quovadisoffshore.com/crl/issuing_ca_name.crl) or is made available via Online Certificate Status Protocol checking ([www.ocsp.quovadisoffshore.com](http://www.ocsp.quovadisoffshore.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**

Key Archive is an optional feature and must be requested by the Digital Certificate Holder before the Digital Certificate is generated.

#### **4.11. End Of Subscription**

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

- Allowing a Digital Certificate to expire without renewing the Digital Certificate.
- Revoking a Digital Certificate without renewing it.

#### **4.12. Key Archival And Recovery**

The QuoVadis PKI only provides key archival for enterprise customers and their employees for purposes of data recovery.

##### **4.12.1. Key Archival And Recovery Policy And Practices**

Key archival and recovery practices and procedures are as specified in agreements with enterprise customers.

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

Not Applicable.

### **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 wherever those operations physically occur.

##### **5.1.1. Site Location and construction**

QuoVadis performs its CA operations from a secure datacentre located in an office complex in Bermuda. The QuoVadis datacentre meets the standards of an independent security certification body at a highly protected level. Standards and protections include: certified BS-EN 1047 performance, backed by ISO9000/1/2 liability insurance; fire (according to DIN 4102 F90) with an automatic FM200 extinguishing system; smoke and humidity (according to DIN 18095); burglary and vandalism (ET2 according to DIN 18103); and protection against electromagnetic influences and radiation (such as electromagnetic pulse).

##### **5.1.2. Physical Access**

QuoVadis permits entry to its secure operating area only to security-cleared and authorised personnel, whose movements within the facility are logged and audited. Physical access is controlled by a combination of physical access cards and biometric readers.

##### **5.1.3. Power And Air-Conditioning**

The QuoVadis secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure. Automatic failover to standby generators is provided.

##### **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, and the enclosure meets the requirements of DIN 18095.

### 5.1.5. Fire Prevention And Protection

The QuoVadis secure operating area provides protection against fire according to DIN 4102 F90 with an automatic FM200 extinguishing system.

### 5.1.6. Media Storage

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

### 5.1.7. Waste Disposal

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

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

### 5.1.8. Off-Site Backup

An off-site location is used for the storage and retention of backup software and data. The off-site storage:

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

## 5.2. Procedural Controls

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

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

It is company policy that QuoVadis will not outsource any of its PKI operations to other 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 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 will be recorded for future reference if needed.
- All data and procedures involved in the certification and distribution of Digital Certificates will be recorded.
- All data relevant to the publication of Digital Certificates and Certificate Revocation Lists will be recorded.
- All Digital Certificate revocation request details are recorded including reason for revocation.
- Certificate and hardware security lifecycle management is recorded.
- Logs recording all network traffic to and from trusted machines are recorded and audited.
- All aspects of the configuration of the backup site are recorded. All procedures involved in the backup process are recorded.
- All data recorded as mentioned in the above sections is backed up. Therefore, there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios.
- All aspects of the installation of new or updated software.
- All aspects of hardware updates.
- All aspects of shutdowns and restarts.
- Time and date of Log Dumps.
- Time and date of Transaction Archive Dumps.
- Security profile changes

All 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 are retained as archive records for a period no less than eleven (11) years for audit trail files, and no less than eleven (11) years for Key and Digital Certificate information. Audit logs are stored until at least eleven (11) years after the QuoVadis Issuing Certification Authority ceases operation.

**5.4.4. Protection Of Audit Log**

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

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

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

**5.4.5. Audit Log Backup Procedures**

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

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

**5.4.6. Audit Collection System**

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

**5.4.7. Notification To Event-Causing Subject**

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

**5.4.8. Vulnerability Assessment**

Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the QuoVadis 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 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, use, revocation, expiration, and renewal activities. 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;
- Digital Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- 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**

QuoVadis Issuing Certification Authority archives will be retained and protected against modification or destruction for a period of eleven (11) years.

**5.5.3. Protection Of Archive**

Archives shall be retained and protected against modification or destruction. Only Certification Authority Officers, the QuoVadis Chief Security Officer, 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 all of its records. All events that are recorded within the QuoVadis Service include the date and time of when the event took place. This date and time are based on the system time on which the CA system is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis PKI rely on a trusted time source.

**5.5.6. Archive Collection System**

The QuoVadis Archive Collection System is internal. QuoVadis provides assistance to Issuing Certification Authorities and Registration Authorities within the QuoVadis PKI to preserve their audit trails.

**5.5.7. Procedures To Obtain And Verify Archive Information**

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

**5.6. Key Changeover**

Key changeover is not automatic, but procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA private key's lifetime, QuoVadis ceases using its expiring CA private key to sign Certificates (well in advance of expiration) and uses the old private key only to sign CRLs 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 Digital Certificate Holders, Authorised Relying Parties, and other relevant parties in the QuoVadis PKI;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained; and
- notify relevant Government and Certification bodies under applicable laws and related regulations.

For Qualified Certificates, in accordance with Swiss Digital Signature law, a notice of termination of the Issuing CA must be communicated in accordance with pre-established procedures to SAS, the body responsible for accrediting the Certificate Service Provider.

#### **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 Federal Information Processing Standard-140 level 4 and 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.

### **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 Digital Certificate Holder's public and private key pair. The Digital 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 Digital Certificate Holder's public and private key pair are generated within a secure environment. QuoVadis Digital 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.

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

All Keys for Issuing CAs, Registration Authorities and Registration Authority Officers must be randomly generated on an approved cryptographic token. 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, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a Token for local Key generation at the point of Digital Certificate issuance or request. Offline means will include Identity checking and will not inhibit establishing proof-of-possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a Certificate Holder Agreement or other agreement. In those cases where Key Pairs are generated by the Issuing CA on behalf of the Holder, the Issuing CA will implement secure mechanisms to ensure that the Token on which the Key Pair is held is securely sent to the proper Holder, and that the Token is not activated prior to receipt by the proper Holder.

#### **6.1.4. Certification Authority Public Key To Relying Parties**

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

#### **6.1.5. Key Sizes**

Key lengths within the QuoVadis PKI are determined by Digital Certificate Profiles more fully disclosed in Appendix A. The QuoVadis Issuing CA uses an RSA minimum key length of 1,024-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 PKI are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this QuoVadis CP/CPS. Without limitation to the generality of the foregoing, all participants in the QuoVadis PKI must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised use of their Private Key (to include password, Token or other activation data used to control access to the Private Key); and (ii) exercise sole and complete control and use of the Private Key that corresponds to their Public Key.

**6.2.1. Cryptographic Module Standards And Controls**

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

For Qualified Certificates, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 standards.

**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 Digital Certificate Holder or Registration Authority specifically contracts for such services. Private Keys for signing will not be archived.

Where a single key pair is generated for signing and encryption, the Private Key will only be archived on the specific request of the Digital Certificate Holder and the corporate entity with which that Digital Certificate Holder is affiliated.

Under no circumstances will private keys for Qualified Digital Certificates be archived.

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

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

**6.2.7. Private Key Storage On Cryptographic Module**

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

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

#### **6.2.11. Cryptographic Module Rating**

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

For Qualified Certificates, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 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 Public Key Infrastructure are:

- Root CA certificate 25 years
  - All Issuing CA certificates 10 years
  - Qualified Certificates 1 to 3 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**

#### **6.5.1. Specific Computer Security Technical Requirements**

Each Issuing CA must establish an approved System Security Policy that incorporates computer security technical requirements that are specific to that Issuing CA's operations.

The QuoVadis Issuing CA has established an approved System Security Policy that incorporates computer security technical requirements that are specific to QuoVadis and configured to allow the minimal amount of connectivity identified as being necessary to accomplish Certification Authority and Registration Authority functions.

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 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**

QuoVadis has established an approved System Security Policy that incorporates computer security ratings that are specific to QuoVadis.

QuoVadis computer security ratings are achieved and maintained by real-time security monitoring and analysis, monthly security reviews by the QuoVadis Chief Security Officer and annual security reviews by external auditors.

### **6.6. Life Cycle Technical Controls**

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

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

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

#### **6.6.1. System Development Controls**

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

### 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 public key 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.

### 6.8. Time-Stamping

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

The QuoVadis Time-stamp Policy aims to deliver time-stamping services used in support of qualified electronic signatures, (i.e. in line with article 5.1 of the European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures), as well as under applicable Swiss and Bermuda law and regulations. However QuoVadis Time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The structure and content of the QuoVadis Time-stamp Policy is in accordance with ETSI TS 101.023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities. The QuoVadis Time-stamp Policy is administered and approved by the QuoVadis Policy Management Authority and should be read in conjunction with this CP/CPS.

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1. Certificate Profile

All QuoVadis Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 3280 and utilise the ITU-T X.509 version 3 Digital Certificate standard.

Digital Certificate profiles within the QuoVadis PKI are detailed in Appendix A.

#### 7.1.1. Version Numbers

Digital Certificates in the QuoVadis PKI are x.509 Version 3

#### 7.1.2. Certificate Extensions

Digital Certificate Extensions are stipulated in the Digital Certificate Profiles detailed in Appendix A.

**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 are 1.3.6.1.4.1.8024.0.1 and 1.3.6.1.4.1.8024.0.3.

**7.1.7. Usage Of Policy Constraints Extension**

No Stipulation.

**7.1.8. Policy Qualifiers Syntax And Semantics**

Digital Certificates issued within the QuoVadis PKI contain one of the Object Identifiers for this CP/CPS.

**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 3280.

**7.2.1. Version Number**

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

**7.2.2. Certificate Revocation List And Certificate Revocation List Entry Extensions**

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

**7.3. Online Certificate Status Protocol Profile**

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

**7.3.1. Online Certificate Status Protocol Version Numbers**

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

**7.3.2. Online Certificate Status Protocol Extensions**

No Stipulation.

**7.4. Lightweight Directory Access Protocol Profile**

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

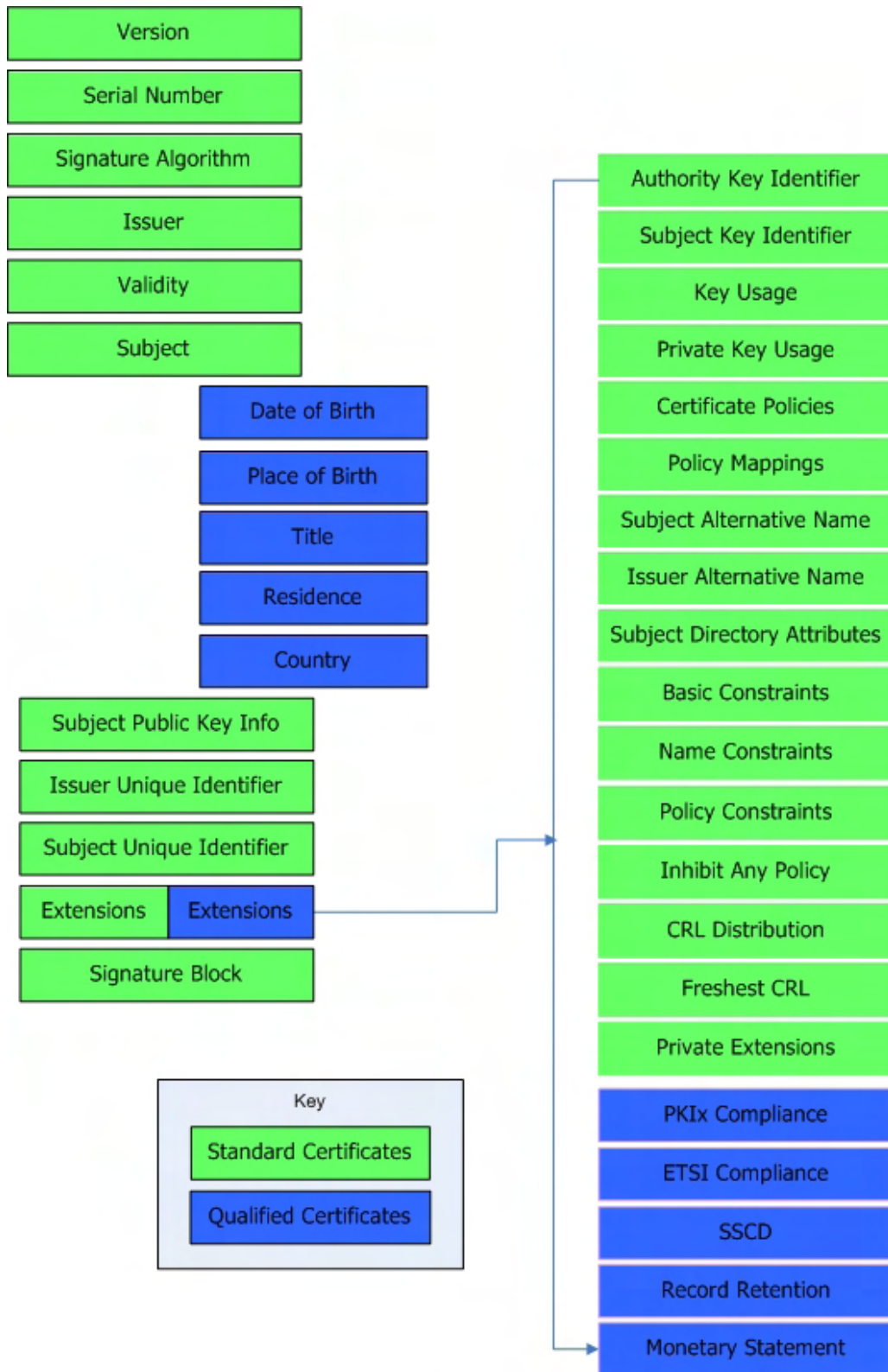
**7.4.1. Lightweight Directory Access Protocol Version Numbers**

LDAP V3 in accordance with RFC-3377

**7.4.2. Lightweight Directory Access Protocol Extensions**

No Stipulation.

7.5. Root And Issuing Certification Authority Profiles And Certificate Fields  
 7.5.1. Digital Certificate Fields



7.5.1.1. QuoVadis Root Certification Authority Certificate Profile

Field	QuoVadis Root Certificate Profile
Version	3
Serial Number	3ab6508b
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Validity	NotBefore: 3/19/2001 2:33 PM NotAfter: 3/17/2021 2:33 PM
Subject	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Subject Public Key Info.	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	Certificate Extensions: 6 1.3.6.1.5.5.7.1.1: Flags = 0, Length = 31 Authority Information Access [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://ocsp.quovadisoffshore.com  2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None  2.5.29.32: Flags = 0, Length = 111 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certification practices, and the QuoVadis Certificate Policy.  [1,2]Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: http://www.quovadis.bm  2.5.29.14: Flags = 0, Length = 16 Subject Key Identifier: 8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df  2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority OU=Root Certification Authority

Field	QuoVadis Root Certificate Profile
	O=QuoVadis Limited C=BM Certificate SerialNumber=3a b6 50 8b  2.5.29.15: Flags = 1(Critical), Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06) Signature Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer  Key Id Hash (sha1): 86 26 cb 1b c5 54 b3 9f bd 6b ed 63 7f b9 89 a9 80 f1 f4 8a Subject Key Id (precomputed): 8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Cert Hash(md5): 27 de 36 fe 72 b7 00 03 00 9d f4 f0 1e 6c 04 24 Cert Hash sha1): de 3f 40 bd 50 93 d3 9b 6c 60 f6 da bc 07 62 01 00 89 76 c9

7.5.1.2. QuoVadis Issuing CA 2: Bermuda Jurisdiction – Non Qualified Digital Certificates

Field	QuoVadis Issuing CA 2
Version	3
Serial Number	3ce07ab9
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Validity	NotBefore: 5/13/2002 10:47 PM NotAfter: 5/10/2012 10:47 PM
Subject	CN=QuoVadis Issuing Certification Authority 2 OU=Issuing Certification Authority O=QuoVadis Limited C=BM
Subject Public Key Info.	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	Certificate Extensions: 7 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None  2.5.29.15: Flags = 1(Critical), Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06)  2.5.29.32: Flags = 0, Length = 111 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certification practices, and the QuoVadis Certificate Policy. [1,2] Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: <a href="http://www.quovadis.bm">http://www.quovadis.bm</a>

Field	QuoVadis Issuing CA 2
	<p>1.3.6.1.5.5.7.1.1: Flags = 0, Length = 6e                      Authority Information Access                      [1]Authority Info Access      Access Method=On-line Certificate Status Protocol                      (1.3.6.1.5.5.7.48.1)                      Alternative Name:              URL=https://ocsp.quovadisoffshore.com                      [2]Authority Info Access      Access Method=Certification Authority Issuer                      (1.3.6.1.5.5.7.48.2)                      Alternative Name:              URL=http://www.quovadisoffshore.com/trust/qvrca.crt</p> <p>2.5.29.31: Flags = 0, Length = 37                      CRL Distribution Points                      [1]CRL Distribution Point                      Distribution Point Name:      Full Name:                      URL=http://www.quovadisoffshore.com/crl/qvrca.crl</p> <p>2.5.29.35: Flags = 0, Length = a6                      Authority Key Identifier      KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84                      6a cb ef df                      Certificate Issuer:                      Directory Address:              CN=QuoVadis Root Certification Authority                      OU=Root Certification Authority                      O=QuoVadis Limited                      C=BM                      Certificate SerialNumber=3a b6 50 8b</p> <p>2.5.29.14: Flags = 0, Length = 16                      Subject Key Identifier      a4 14 d3 93 16 26 26 49 3b 0c a3 81 5f 75 1e b7 b3 8d 04 eb</p> <p>Signature Algorithm:      Algorithm ObjectId:      1.2.840.113549.1.1.5      sha1RSA                      Algorithm Parameters:      05 00</p>
Signature Block	<p>Non-root Certificate</p> <p>Key Id Hash(sha1): da 3d c3 2a be 3c 79 c1 7b 4b 8e 53 f3 93 e2 5d fd df 60 38                      Subject Key Id (precomputed): a4 14 d3 93 16 26 26 49 3b 0c a3 81 5f 75 1e b7 b3 8d 04 eb                      Cert Hash(md5): 2a 67 5e 90 93 fd 86 d4 27 a8 9e 49 92 23 1f 35                      Cert Hash(sha1): 13 0c 8e 32 20 cb e3 b8 a9 00 39 81 db 4d eb 8a fe 99 de e6</p>

7.5.1.3. QuoVadis Issuing CA 3 and QuoVadis Qualified Issuing CA 1: Swiss Jurisdiction – Qualified Certificates

Field	QuoVadis Issuing CA 3
Version	3
Serial Number	1109380779
Signature algorithm identifier	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer name	C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority
Period of validity	Not Before: Feb 15 21:46:22 2006 GMT Not After : Feb 15 21:46:22 2016 GMT
Subject name	C=CH O=QuoVadis Limited, Bermuda OU=Issuing Certification Authority CN=QuoVadis ICA 3
Subject's public-key information	Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	<p>Certificate Extensions: 9</p> <p>2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None</p> <p>1.3.6.1.5.5.7.1.1: Flags = 0, Length = 5c Authority Information Access [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://ocsp.quovadis.bm</p> <p>[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.quovadis.bm/trust/qvrca.crt</p> <p>1.3.6.1.5.5.7.1.3: Flags = 1(Critical), Length = 18</p> <p>QC Statements Qualified Digital Certificate id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1)</p> <p>2.5.29.32: Flags = 0, Length = 101 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Reliance on the QuoVadis Root Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the QuoVadis Certificate Policy &amp; Certification Practice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: http://www.quovadis.bm</p> <p>2.5.29.15: Flags = 1(Critical), Length = 4</p>



Field	QuoVadis Issuing CA 3
	Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	2.5.29.18: Flags = 0, Length = 51 Issuer Alternative Name Directory Address: O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA
	2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM Certificate SerialNumber=3a b6 50 8b
	2.5.29.31: Flags = 0, Length = 37 CRL Distribution Points [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.quovadisoffshore.com/crl/qvrca.crl
	2.5.29.14: Flags = 0, Length = 16 Subject Key Identifier 63 dd d3 3d 98 63 f0 4e 1c 56 d5 45 4f 89 84 5b 2f d5 e1 fa
Signature Block	Non-root Certificate Key Id Hash(sha1): 3d c9 01 1f 93 b4 07 09 43 d4 e5 fa 73 9f 84 6d bb 44 8e 09 Subject Key Id (precomputed): 63 dd d3 3d 98 63 f0 4e 1c 56 d5 45 4f 89 84 5b 2f d5 e1 fa Cert Hash(md5): f6 50 cb 09 bc 4d 2f 02 1c 69 1b bd cd 34 30 de Cert Hash(sha1): 4b 1b 8c 2e c0 d2 bc 80 38 ed 2c c3 aa 9a 5f 77 28 dc 41 61

Field	QuoVadis Qualified Issuing CA 1
Version	3
Serial Number	421fd153
Signature algorithm identifier	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer name	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM
Period of validity	Not Before: July 5 20:15:00 2007 GMT Not After : July 5 20:15:00 2017 GMT
Subject name	CN=QuoVadis Qualified Issuing Certification Authority 1 OU=Issuing Certification Authority O=QuoVadis Limited, Bermuda C=CH
Subject's public-key information	Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 2048 bits
Extensions	Certificate Extensions: 8 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA

Field	QuoVadis Qualified Issuing CA 1
	<p>Path Length Constraint=None</p> <p>1.3.6.1.5.5.7.1.1: Flags = 0, Length = 2e                      Authority Information Access                      [1]Authority Info Access                      Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48                      .1)                      Alternative Name:                      URL=http://ocsp.quovadisglobal.com</p> <p>1.3.6.1.5.5.7.1.3: Flags = 0, Length = 18                      Unknown Extension type</p> <p>0000 30 16 30 0a 06 08 2b 06 01 05 05 07 0b 02 30 08 00...+.....0.                      0010 06 06 04 00 8e 46 01 01 .....F..</p> <p>2.5.29.32: Flags = 0, Length = e4                      Certificate Policies                      [1]Certificate Policy:                      Policy Identifier=1.3.6.1.4.1.8024.0.1                      [1,1]Policy Qualifier Info:                      Policy Qualifier Id=User Notice                      Qualifier:                      Notice Text=Reliance on the QuoVadis Root Certificate by                      any party assumes acceptance of the QuoVadis Certificate Policy/Certification Pr                      actice Statement.                      [1,2]Policy Qualifier Info:                      Policy Qualifier Id=CPS                      Qualifier:  <a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a></p> <p>2.5.29.15: Flags = 1(Critical), Length = 4                      Key Usage                      Certificate Signing, Off-line CRL Signing, CRL Signing (06)</p> <p>2.5.29.18: Flags = 0, Length = 51                      Issuer Alternative Name                      Directory Address:                      O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA</p> <p>2.5.29.35: Flags = 0, Length = a6                      Authority Key Identifier                      KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df                      Certificate Issuer:                      Directory Address:                      CN=QuoVadis Root Certification Authority                      OU=Root Certification Authority                      O=QuoVadis Limited                      C=BM                      Certificate SerialNumber=3a b6 50 8b</p> <p>2.5.29.14: Flags = 0, Length = 16                      Subject Key Identifier                      21 f0 05 b5 f8 ae 5e fc 5d 91 46 6b 26 e0 e1 a5 55 c6 c7 a5</p>
Signature Block	<p>Non-root Certificate                      Key Id Hash(sha1): 4e 04 3d d7 ba e5 e0 22 f4 59 39 45 b6 2c 76 17 31 90 eb 6f                      Subject Key Id (precomputed): 21 f0 05 b5 f8 ae 5e fc 5d 91 46 6b 26 e0 e1 a5 55 c6 c7 a5                      Cert Hash(md5): eb a6 a8 64 73 c1 f0 6b 4f 24 08 04 0f c7 e2 a6</p>

Field	QuoVadis Qualified Issuing CA 1
	Cert Hash(sha1): 78 e2 dc c8 30 02 32 cb 15 79 0b 39 9b 23 3b ee 79 a5 c2 39

7.5.1.4. QuoVadis Root CA 3 Certificate Profile

Field	QuoVadis Root CA 3 Profile
Version	3
Serial Number	05c6
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Validity	NotBefore:11/24/2006 3:11:23 PM NotAfter: 11/24/2031 3:06:44 PM
Subject	CN= QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Subject Public Key Info.	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 4096 bits
Extensions	<p>Certificate Extensions: 5</p> <p>2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None</p> <p>2.5.29.32: Flags = 0, Length = d9 Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 3 Certificate Policy / Certification Practice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a></p> <p>2.5.29.15: Flags = 0, Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06)</p> <p>2.5.29.14: Flags = 0, Length = 16 Subject Key Identifier f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0</p> <p>2.5.29.35: Flags = 0, Length = 67 Authority Key Identifier KeyID=f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Certificate Issuer: Directory Address: CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM Certificate SerialNumber=05 c6</p>

Field	QuoVadis Root CA 3 Profile
	Signature Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer  Key Id Hash(sha1): 14 8d b3 54 ed 9b 2f 13 08 7c c3 8b 4b c1 5b 96 8a c5 53 78 Subject Key Id (precomputed): f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Cert Hash(md5): 31 85 3c 62 94 97 63 b9 aa fd 89 4e af 6f e0 cf Cert Hash(sha1): 1f 49 14 f7 d8 74 95 1d dd ae 02 c0 be fd 3a 2d 82 75 51 85

7.5.1.5. QuoVadis Root CA CRL Profile

Field	QuoVadis Root CA CRL
Version	2
Signature	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Issuer	CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited C=BM  CN=QuoVadis Root CA 3 O=QuoVadis Limited C=BM
Validity	ThisUpdate: Month/Day/Year NextUpdate: Month/Day/Year
Extensions	CRL Extensions: 3  2.5.29.20: Flags = 0, Length = 3 CRL Number CRL Number=#  2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df or f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0  Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority or CN=QuoVadis Root CA 3 OU=Root Certification Authority O=QuoVadis Limited O=QuoVadis Limited C=BM C=BM  Certificate SerialNumber=3a b6 50 8b or 05c6  2.5.29.28: Flags = 0, Length = 35 Issuing Distribution Point Distribution Point Name: Full Name: URL=http://www.quovadisoffshore.com/crl/qvrca.crl Only Contains User Certs=No Only Contains CA Certs=No Indirect CRL=No
Signature Block	Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00 CRL Hash(md5): ce ab 91 70 7f db 15 2d e4 6f 88 90 d1 3e 35 19 CRL Hash(sha1): ac 1e f1 0f 8b e0 8a e3 92 0d 4f 01 f7 11 0f 58 6d a4 27 68

**8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**  
**8.1. Frequency, Circumstance And Standards Of Assessment**  
**8.1.1. QuoVadis Certification Authority**

QuoVadis is subject to audits in respect of its various accreditations and certifications as follows:

Standards / Law	
Bermuda Accredited Certificate Service Provider	As defined in Bermuda's Electronic Transactions Act 1999, an Authorised Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.
Webtrust for Certification Authorities	The WebTrust Seal of assurance for Certification Authorities (CA) symbolises to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria.
SR 943.03 [ZertES]	Dated 21 December 2004 Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der (qualifizierten) elektronischen Signatur
SR 943.032 [VZertES]	Dated 6 December 2004 TAV Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur
SR 943.032.1 [TAV]	Dated 6 December 2004 (Ausgabe 1: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur („zur Anerkennung für qualifizierte elektronische Zertifikate“ nach Kapitel 2)
ESI (“Directive”)	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
ETSI [ESTI101456TS]	TS 101 456 v.1.4.1 January 2006 EU Standards Body Technical Specification - Policy Requirements for certification authorities issuing qualified certificates
ETSI [ESTI101862TS]	TS 101 862, v1.3.2 June 2004, Qualified Certificate Profile
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework corrigenda IETF RFC 3647 (including Erratum issued by IETF April 2004)

The results of these audits in the form of such publicly available audit reports as provided by the external auditors responsible for these audits will be published at [www.quovadis.bm/audits](http://www.quovadis.bm/audits). Compliance audits as carried out under these provisions may substitute for audits noted in this CP/CPS.

**8.1.2. Issuing Certification Authorities**

Issuing CAs (including QuoVadis) will undergo an audit in order to determine compliance with this QuoVadis CP/CPS at least annually. These audits shall include the review of all relevant documents maintained by the Issuing CA regarding operations within the QuoVadis PKI and under this QuoVadis CP/CPS, and other related operational policies and procedures.

**8.1.3. Registration Authorities**

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

**8.2. Identity And Qualifications Of Assessor**

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

Ernst & Young. The accreditation audits for Swiss and European signature requirements have been performed by KPMG Klynveld Peat Marwick Goerdeler SA.

### **8.3. Assessor's Relationship To Assessed Entity**

The auditor and the Issuing CA under audit, must not have any other relationship that would impair the auditor's independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

### **8.4. Topics Covered By Assessment**

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

- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;
- Contracts; and
- Privacy Considerations.

### **8.5. Actions Taken As A Result Of Deficiency**

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

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

#### **8.5.1. Issuing Certification Authorities**

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

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

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

#### **8.5.2. Registration Authorities**

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

---

Certificate. Any decision regarding which of these actions to take will be based on QuoVadis' opinion of the severity and materiality of the irregularities.

#### **8.6. Publication Of Audit Results**

The audit opinion based on results of the audits will be generally available upon request. The results of the most recent audit of QuoVadis will be posted in the Repository located at [www.quovadis.bm](http://www.quovadis.bm).

### **9. OTHER BUSINESS AND LEGAL MATTERS**

#### **9.1. Fees**

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

##### **9.1.1. Certificate Issuance Or Renewal Fees**

Fees may be payable with respect to the issue or renewal of Digital Certificates--details of which are contained within the relevant contractual documentation governing the issue or renewal 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 a commercially reasonable manner and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

##### **9.2.1. Insurance Coverage**

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

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

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

##### **9.2.2. Other Assets**

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

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

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

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

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

**9.2.4. Fiduciary Relationships**

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

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

**9.3. Confidentiality Of Business Information****9.3.1. Scope Of Confidential Information**

Any personal or corporate information held by Issuing CAs related to a Digital 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 Digital Certificate Holder or the Digital 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 on 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, Digital 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, Digital 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 Digital 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 Public Key Infrastructure, 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 Digital 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 Digital 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.

For Qualified Certificates issued in accordance with Swiss Digital Signature laws, Certificate Holders expressly consent to personal data in the form of the data included in the Certificate Fields being transferred outside of Switzerland and published in a repository which makes this information publicly available to persons searching the repository with the appropriate query string. Personal data obtained during the registration process which is not included in the Certificate Fields will not be transmitted outside of Switzerland.

**9.4.6. Disclosure Pursuant To Judicial Or Administrative Process****9.4.6.1. Release To Law Enforcement Officials**

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

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

**9.4.6.2. Release As Part Of Civil Discovery**

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

determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the relevant CA and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the CA (e.g. those of the relevant EU Member).

#### **9.4.7. Other Information Disclosure Circumstances**

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

#### **9.5. Intellectual Property Rights**

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

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 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, copyright in, and the right to license this QuoVadis CP/CPS.

##### **9.5.1. Object Identifiers**

Copyright in the Object Identifiers for the QuoVadis infrastructure vests solely in QuoVadis.

##### **9.5.2. Licences**

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

##### **9.5.3. IETF Guidelines**

The use of the PKIX IETF Guidelines is acknowledged.

##### **9.5.4. Breach**

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

#### **9.6. Representations And Warranties**

##### **9.6.1. Certification Authority Representations**

###### **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 Root Certification Authority Hash at [www.quovadis.bm](http://www.quovadis.bm) 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 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 (a) it has taken reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue, and (b) 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 nature of the steps the Issuing CA takes to verify the information contained in a Digital Certificate vary according to the Digital Certificate fee charged, the nature and identity of the Digital Certificate Holder, and the applications for which the Digital Certificate will be marked as trusted. 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 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**

Digital Certificate Holders represent and warrant that:

- The Private Key is protected and has never been accessed by another person.
- All representations made by the Digital 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.

## **9.6.4. Relying Parties Representations And Warranties**

Relying Parties represent and warrant that:

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

## **9.6.5. Representations And Warranties Of Other Participants**

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

**9.7. Disclaimers Of Warranties**

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

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

**9.8. Liability and Limitations of Liability****9.8.1. QuoVadis Liability**

QuoVadis shall be liable to Digital 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). 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.

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

1. QuoVadis is liable to the Certificate Holder or the Relying Party who relies on a valid Qualified Certificate, for damages that arise because QuoVadis has not followed the procedures required by ZertES.
2. QuoVadis has the obligation to prove that such procedures were followed in accordance with ZertES.
3. QuoVadis cannot disclaim liability to either the Certificate Holder or Relying Party except where the Certificate Holder or Relying Party has not complied with the terms and conditions of use of the Certificate.

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

**9.8.2. QuoVadis' Limitations Of Liability**

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

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

For the avoidance of doubt, QuoVadis shall bear no liability or responsibility to any person that participates in the QuoVadis PKI unless that person is a Holder.

**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
Standard Certificates	\$100,000.00
Device Certificate	\$100,000.00

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

### **9.11. Individual Notices And Communications With Participants**

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

### **9.12. Amendments**

#### **9.12.1. Procedure For Amendment**

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

There are two possible types of policy change:

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

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

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

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

#### **9.12.2. Notification Mechanism And Period**

New or amended CP/CPSs are published on the web site [www.quovadis.bm/policies](http://www.quovadis.bm/policies).

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; no provision is made for different versions of this CP/CPS to remain in effect at the same time.

\* 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 PKI (for these purposes, QuoVadis shall be deemed a "participant" within the QuoVadis PKI) arising out of or relating to this QuoVadis CP/CPS shall be referred to an arbitration tribunal.

For Qualified Certificates, in accordance with the Swiss Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in Switzerland.

#### **9.14. Governing Law**

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

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

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

**9.15. Compliance With Applicable Law**

This CP/CPS is subject to applicable law.

**9.16. Miscellaneous Provisions**

Not Applicable.

**9.16.1. Entire Agreement**

Not Applicable.

**9.16.2. Assignment**

Not Applicable.

**9.16.3. Severability**

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

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

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

**9.16.5. Force Majeure**

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

**9.17. Other Provisions**

No Stipulation.

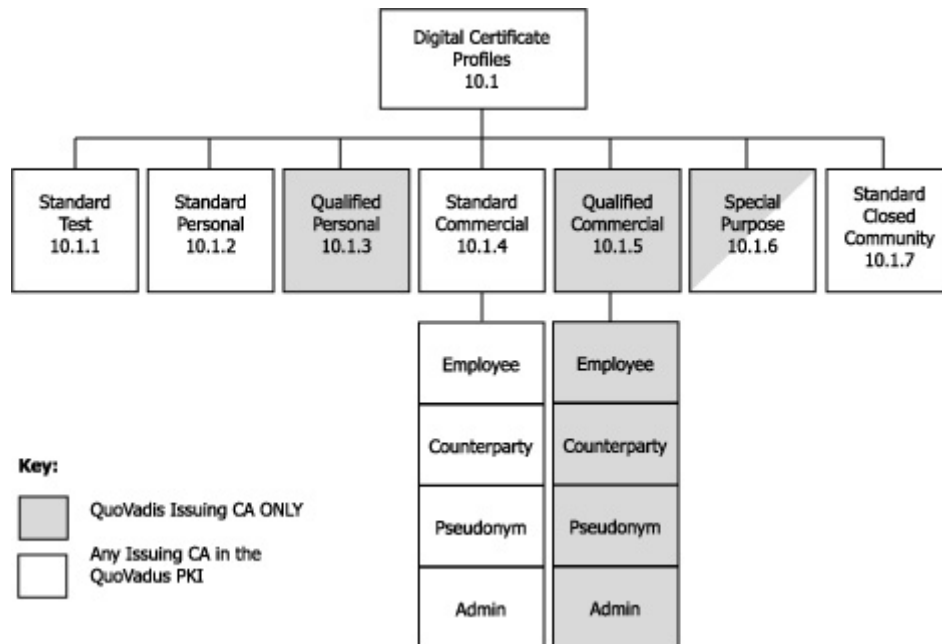


**10. APPENDIX A**  
**10.1. Digital Certificate Profiles**

Within the QuoVadis PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. All Digital Certificate Profiles within the QuoVadis PKI are detailed below, (See Diagram 3 and corresponding subsections below).

The procedure for Digital Certificate Holder registration, Digital Certificate generation and distribution is 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 customers.

Please note that where a Qualified Digital Certificate is issued within the meaning of European Union Directive 199/93/EC, the individual applying for the Qualified Digital Certificate must undergo a face-to-face identification and verification procedure.



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

10.1.1. Standard Test Certificate

<b>INITIAL REGISTRATION</b>		
<ul style="list-style-type: none"> <li>Issued by approved Issuing CAs in the QuoVadis PKI.</li> <li>Registration performed by approved Registration Authorities in the QuoVadis PKI.</li> </ul>		
<b>IDENTIFICATION &amp; AUTHENTICATION</b>		
There is no formal Identification & Authentication requirement for Standard Test Digital Certificates. Standard Test Digital Certificates are issued for limited duration on the basis of the Applicant Digital Certificate Holder's self certification.		
<b>REGISTRATION PROCESS</b>		
Registration information may be received from an Applicant Digital Certificate Holder:		
<ul style="list-style-type: none"> <li>In person, or</li> <li>By mail or electronic methods</li> </ul>		
Standard Test Digital Certificates Holders participate in the QuoVadis PKI. Issued to Digital Certificate Holders based on non-certified forms of identification; designated as a No-Reliance Digital Certificate. A Registration Authority Officer collects Digital Certificate Holder details during the Application process ensuring that the information supplied is correct. During the registration process, it is a requirement for an Applicant Digital Certificate Holder to accept the Certificate Holder agreement. The Certificate Holder Agreement details the terms and conditions under which the Digital Certificate is being supplied including the Digital Certificate Holder's rights and obligations.		
<b>DIGITAL CERTIFICATE GENERATION</b>		
All successful Standard Test Digital Certificate requests will be processed by the Issuing CA. Each Standard Test Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The Issuing CA will apply to the Digital Certificate request a:		
<ul style="list-style-type: none"> <li>Unique serial number</li> <li>Operational Certification Authority's signature</li> </ul>		
<b>DIGITAL CERTIFICATE DELIVERY</b>		
<ul style="list-style-type: none"> <li>Download over the Internet</li> <li>CD/Floppy Disk</li> <li>Smart Card or other secure hardware token</li> <li>E-mail</li> </ul>		
<b>FIELDS</b>	<b>CONTENT</b>	<b>DEMARICATION</b>
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	Sha1RSA	Fixed
<b>Issuer</b>		
Common Name (CN)	Issuing Certification Authority Name	ICA Variable
Organisational Unit (OU)	Issuing Certification Authority	ICA Variable
Organisation (O)	Company Name	ICA Variable
Country (C)	Issuing Certification Authority Jurisdiction	ICA Variable
Valid From	MM/DD/YYYY HH:MM A.M/P.M	ICA Variable
Valid To	MM/DD/YYYY HH:MM A.M/P.M	ICA Variable
<b>Subject</b>		
Email Address (E)	<a href="mailto:aaa@bbb.xx.yy">aaa@bbb.xx.yy</a> or <a href="mailto:aaa@bbb.com">aaa@bbb.com</a>	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Standard Test	Fixed
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisation (O)	QuoVadis Trust Services	
Country/Locality	Variable Data	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Issuer Unique Identifier	Special Application	ICA Variable
Subject Unique Identifier	Special Application	CH Variable
<b>Extensions</b>		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature (Optional)	CH Variable
Key Usage	Key Encipherment (Optional)	CH Variable

---

Key Usage	Data Encipherment (Optional)	CH Variable
Key Usage	Key Agreement (Optional)	CH Variable
Enhanced Key Usage	Client Authentication (Optional)	CH Variable
Enhanced Key Usage	Secure Email (Optional)	CH Variable
Enhanced Key Usage	Encrypting File System (Optional)	CH Variable
Enhanced Key Usage	Smart Card Logon (Optional)	CH Variable
Certificate Policies	<a href="http://www.quovadis.bm/pn">http://www.quovadis.bm/pn</a>	Fixed
Authority Information Access	<a href="https://www.ocsp.quovadisoffshore.com">https://www.ocsp.quovadisoffshore.com</a>	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	<a href="http://www.ocsp.quovadisoffshore.com/crl/CAname.crl">http://www.ocsp.quovadisoffshore.com/crl/CAname.crl</a>	Fixed
Private Extensions	Special Application	CH Variable
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	<a href="http://www.quovadis.bm/policies">www.quovadis.bm/policies</a>	Fixed

10.1.2 Standard Personal Certificate

<b>INITIAL REGISTRATION</b>		
<ul style="list-style-type: none"> <li>Issued by the QuoVadis Issuing CA.</li> <li>Registration performed by QuoVadis Registration Authorities.</li> </ul>		
<b>IDENTIFICATION &amp; AUTHENTICATION</b>		
Accredited Digital Certificate under the Bermuda Certification Service Provider Legislation, issued to Applicant Digital Certificate Holders based on the in-person presentation of required identification to a QuoVadis Registration Authority.		
<b>REGISTRATION PROCESS</b>		
<p>A QuoVadis Registration Authority Officer verifies that the Government issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (<i>e.g.</i>, holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:</p> <ul style="list-style-type: none"> <li>in person or</li> <li>by mail or electronic methods.</li> </ul> <p>The Registration and Authentication process of a Standard Personal Digital Certificate Holder's identity includes:</p> <ul style="list-style-type: none"> <li>the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.</li> <li>one form of government issued photographic identification is reviewed and photocopied.</li> <li>one additional form of identification, the name on which corresponds to the name that appears on the government issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.</li> </ul>		
<b>DIGITAL CERTIFICATE GENERATION</b>		
<p>All successful Standard Personal Digital Certificate requests will be processed by the QuoVadis Issuing Certification Authority. Each Standard Personal Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The QuoVadis Issuing Certification Authority will apply to the Digital Certificate request a:</p> <ul style="list-style-type: none"> <li>Unique serial number</li> <li>Operational Certification Authority's signature</li> </ul>		
<b>DIGITAL CERTIFICATE DELIVERY</b>		
<ul style="list-style-type: none"> <li>Download over the Internet</li> <li>CD/Floppy Disk</li> <li>Smart Card or other secure hardware token</li> </ul> <p>Certificate Pins are delivered in an out of band manner to the physical delivery method used for the Certificate.</p>		
<b>FIELDS</b>	<b>CONTENT</b>	<b>DEMARICATION</b>
<b>Version</b>	Version 3	Fixed
<b>Serial Number</b>	Unique Number System Generated	Fixed
<b>Signature Algorithm</b>	Sha1RSA	Fixed
<b>Issuer</b>		
Common Name (CN)	Issuing Certification Authority Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Company Name	Fixed
Country (C)	Issuing Certification Authority Jurisdiction	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
<b>Subject</b>		
Email Address (E)	<a href="#">aaa@bbb.xx.yy</a> or <a href="#">aaa@bbb.com</a>	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Standard Personal	Fixed
Organisational Unit (OU)	Variable Data	CH Variable
Organisational Unit (OU)	Variable Data	CH Variable
Organisation (O)	QuoVadis Trust Services	Fixed
Country/Locality	Variable Data	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Subject Unique Identifier	Special Application	CH Variable
<b>Extensions</b>		

Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature (Optional)	CH Variable
Key Usage	Non Repudiation (Optional)	CH Variable
Key Usage	Key Encipherment (Optional)	CH Variable
Key Usage	Data Encipherment (Optional)	CH Variable
Key Usage	Key Agreement (Optional)	CH Variable
Enhanced Key Usage	Client Authentication (Optional)	CH Variable
Enhanced Key Usage	Secure Email (Optional)	CH Variable
Enhanced Key Usage	Encrypting File System (Optional)	CH Variable
Enhanced Key Usage	Smart Card Logon (Optional)	CH Variable
Certificate Policies	<a href="http://www.quovadis.bm/pn">http://www.quovadis.bm/pn</a>	Fixed
Authority Information Access	<a href="https://www.ocsp.quovadisoffshore.com">https://www.ocsp.quovadisoffshore.com</a>	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	<a href="http://www.ocsp.quovadisoffshore.com/crl/CAname.crl">http://www.ocsp.quovadisoffshore.com/crl/CAname.crl</a>	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	<a href="http://www.quovadis.bm/policies">www.quovadis.bm/policies</a>	Fixed

**10.1.3 Qualified Certificate**

Please note that where a Qualified Personal Digital Certificate is issued within the meaning of EU Directive 199/93/EC, the individual applying for the Qualified Personal Digital Certificate must undergo a face-to-face identity verification procedure.

<b>INITIAL REGISTRATION</b>		
<ul style="list-style-type: none"> <li>Issued by QuoVadis Issuing CA.</li> <li>Registration performed by a QuoVadis Registration Authorities.</li> </ul>		
<b>IDENTIFICATION &amp; AUTHENTICATION</b>		
<p>The purpose of a Qualified Personal Digital Certificate is to identify a person with a high level of assurance, where the Qualified Personal 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.</p>		
<b>REGISTRATION PROCESS</b>		
<p>A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (<i>e.g.</i>, holographic devices). The applicant certificate holder must present original documentation in person during a face-to-face verification procedure.</p> <p>The Registration and Authentication process of a Qualified Personal Digital Certificate Holder's identity includes:</p> <ul style="list-style-type: none"> <li>the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority with either a valid Passport or Government-issued Identification Card.</li> <li>one form of government-issued photographic identification is reviewed and photocopied.</li> <li>one additional form of identification, the name on which corresponds to the name that appears on the government-issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.</li> <li>All information on the applicant form and all certificate fields shown in the certificate are verified as accurate.</li> </ul>		
<b>DIGITAL CERTIFICATE GENERATION</b>		
<p>All successful Qualified Personal Digital Certificate requests will be processed by the QuoVadis Issuing CA. Each Standard Personal Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The QuoVadis Issuing CA will apply to the Digital Certificate request a:</p> <ul style="list-style-type: none"> <li>Unique serial number</li> <li>Operational Certification Authority's signature</li> <li>Digital Certificate is generated and stored in a compliant S.S.C.D container - i.e. a secure/cryptographic smartcard or USB token.</li> </ul>		
<b>DIGITAL CERTIFICATE DELIVERY</b>		
<p>Delivered and stored in a compliant S.S.C.D container - i.e. a secure/cryptographic smartcard or USB token. The Certificate Pin is delivered in an out of band manner to the physical delivery method used for the Certificate.</p>		
<b>FIELDS</b>	<b>CONTENT</b>	<b>DEMARICATION</b>
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	Sha1RSA	Fixed
Issuer		Fixed
Common Name (CN)	Issuing Certification Authority Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Company Name	Fixed
Country (C)	Issuing Certification Authority Jurisdiction	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Email Address (E)	<a href="mailto:aaa@bbb.xx.yy">aaa@bbb.xx.yy</a> or <a href="mailto:aaa@bbb.com">aaa@bbb.com</a>	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Not Stipulated	Fixed
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Qualified Certificate	CH Variable
Organisation (O)	Organisation Name	CH Variable
Locality (L)	Not Stipulated	CH Variable
State or Province	Not Stipulated	CH Variable
Country	ISO Country Code	CH Variable

Date Of Birth	DD/MM/YYYY	CH Variable
Place of Birth	City	CH Variable
Gender	M/F	CH Variable
Title	Verified Legal Title	CH Variable
Country of Residence	ISO Country Code – Normally Resident	CH Variable
Country of Citizenship	ISO Country Code – Nationality	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
<b>Extensions</b>		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature Non Repudiation	CH Variable Fixed
Private Key Usage	Validity of Private Key < Cert	CH Variable
Certificate Policies	<a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a>	Fixed
Authority Information Access	<a href="http://ocsp.quovadisglobal.com">http://ocsp.quovadisglobal.com</a>	Fixed
Subject Alternative Name	Principal Name = Email Address	CH Variable
Issuer Alternative Name	O=ZertES Recognition Body KPMG Klynveld Peat Marwick Goerdeler SA	Fixed
QC Statement PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed
QC Statement ETSI Compliance	0.4.0.1862.1.1	Fixed
Monetary Statement	0.4.0.1862.1.2 Max Amount 2 CHF Exponent 6 (CHF 2,000,000)	CH Variable
SSCD Statement	0.4.0.1862.1.4	Fixed
CRL Distribution	<a href="http://crl.quovadisglobal.com/qvqica1.crl">http://crl.quovadisglobal.com/qvqica1.crl</a>	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	<a href="http://www.quovadisglobal.com/cps">www.quovadisglobal.com/cps</a>	Fixed

10.1.4. Standard Commercial Certificate

<b>INITIAL REGISTRATION</b>		
<ul style="list-style-type: none"> <li>Issued by approved Issuing CAs in the QuoVadis PKI.</li> <li>Registration performed by approved Registration Authorities in the QuoVadis PKI.</li> </ul>		
<b>IDENTIFICATION &amp; AUTHENTICATION</b>		
Accredited Digital Certificate under the Bermuda Certification Service Provider Legislation, issued to Applicant Digital Certificate Holders based on the applying Certificate Holder's contractual relationship to the company that operates the Nominating Registration Authority, or its respective subsidiaries and holding companies.		
<b>REGISTRATION PROCESS</b>		
<p>A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (<i>e.g.</i>, holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:</p> <ul style="list-style-type: none"> <li>in person or</li> <li>by mail or electronic methods.</li> </ul> <p>The Registration and Authentication process of a Standard Commercial Digital Certificate Holder's identity includes:</p> <ul style="list-style-type: none"> <li>the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.</li> <li>one form of government-issued photographic identification is reviewed and photocopied.</li> <li>one additional form of identification, the name on which corresponds to the name that appears on the government issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.</li> </ul>		
<b>DIGITAL CERTIFICATE GENERATION</b>		
<p>All successful Standard Commercial Digital Certificate requests will be processed by the Issuing CA. Each Standard Commercial Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The Issuing CA will apply to the Digital Certificate request a:</p> <ul style="list-style-type: none"> <li>Unique serial number</li> <li>Operational Certification Authority's signature</li> </ul>		
<b>DIGITAL CERTIFICATE DELIVERY</b>		
<ul style="list-style-type: none"> <li>Download over the Internet</li> <li>CD/Floppy Disk</li> <li>Smart Card or other secure hardware token</li> </ul> <p>Certificate Pins are delivered in an out of band manner to the physical delivery method used for the Certificate and the Registration Authority may employ the use of a shared secret to identify the Applicant certificate holder during the certificate delivery process.</p>		
<b>FIELDS</b>	<b>CONTENT</b>	<b>DEMARICATION</b>
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	Sha1RSA	Fixed
Issuer		
Common Name (CN)	Issuing Certification Authority Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Company Name	Fixed
Country (C)	Issuing Certification Authority Jurisdiction	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Email Address (E)	<a href="mailto:aaa@bbb.xx.yy">aaa@bbb.xx.yy</a> or <a href="mailto:aaa@bbb.com">aaa@bbb.com</a>	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Standard Commercial	Fixed
Organisational Unit (OU)	Corporate Affiliation – Employee	Fixed
	-or-	
	Corporate Affiliation - Counterparty	Fixed
	-or-	
	Corporate Affiliation - Pseudonymous	Fixed
	-or-	
	Corporate Affiliation - Administrative	Fixed
Organisational Unit (OU)	Not Stipulated	CH Variable



Organisation (O)	QuoVadis Trust Services	Fixed
Country/Locality	Variable Data	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
<b>Extensions</b>		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	CH Variable
Key Usage	Digital Signature (Optional)	CH Variable
Key Usage	Non Repudiation (Optional)	CH Variable
Key Usage	Key Encipherment (Optional)	CH Variable
Key Usage	Data Encipherment (Optional)	CH Variable
Key Usage	Key Agreement (Optional)	CH Variable
Enhanced Key Usage	Client Authentication (Optional)	CH Variable
Enhanced Key Usage	Secure Email (Optional)	CH Variable
Enhanced Key Usage	Encrypting File System (Optional)	CH Variable
Enhanced Key Usage	Smart Card Logon (Optional)	CH Variable
Certificate Policies	<a href="http://www.quovadis.bm/pn">http://www.quovadis.bm/pn</a>	Fixed
Authority Information Access	<a href="https://www.ocsp.quovadisoffshore.com">https://www.ocsp.quovadisoffshore.com</a>	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	<a href="http://www.ocsp.quovadisoffshore.com/crl/CAname.crl">http://www.ocsp.quovadisoffshore.com/crl/CAname.crl</a>	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	<a href="http://www.quovadis.bm/policies">www.quovadis.bm/policies</a>	Fixed

**10.1.5 Commercial - EIDI-V Certificates**

A Commercial Advanced Certificate enables an authorised person or a commercial entity directly associated with a secure signature creation device in conformity with EIDI-V (SR 641.201.1 and SR 641.201.1.1) to digitally sign with the secure signature creation device (SSCD).

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

<b>INITIAL REGISTRATION</b>		
<ul style="list-style-type: none"> <li>Issued by QuoVadis Issuing CA.</li> <li>Registration performed by a QuoVadis Registration Authority.</li> </ul>		
<b>PURPOSE</b>		
The purpose of a Commercial Advanced Digital Certificate is to identify the organisation and individual responsible for creation of signatures under SR 641.201.1 and SR 641.201.1.1.		
<b>REGISTRATION PROCESS</b>		
<p>A QuoVadis Registration Authority Officer verifies that the Government-issued photographic identification presented corresponds to the form of identification issued by that jurisdiction, and that the identification possesses all stated security and anti-fraud features of that form of identification (<i>e.g.</i>, holographic devices). The applicant certificate holder must present original documentation in person during a face-to-face verification procedure. The Registration and Authentication process of a Qualified Commercial Digital Certificate Holder's identity includes: The Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority with either a valid Passport or Government-issued Identification Card.</p> <p>During the Registration process one form of government issued photographic identification is reviewed and photocopied and one additional form of identification, the name on which corresponds to the name that appears on the government-issued photographic identification and the address on which corresponds to the address that appears on the Digital Certificate Holder's application details is reviewed and photocopied.</p> <p>All information on the applicant form and all certificate fields shown in the certificate are verified as accurate. For a commercial entity, (company, partnership, sole trader etc.) The Registration Authority must seek positive assurance regarding the details listed in the certificate by reference to the appropriate official register for that company type.</p>		
<b>DIGITAL CERTIFICATE GENERATION</b>		
<p>All successful Commercial Digital Certificate requests will be processed by the QuoVadis Issuing CA. Each certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The QuoVadis Issuing CA will apply to the Digital Certificate request a:</p> <ul style="list-style-type: none"> <li>Unique serial number</li> <li>Operational Certification Authority's signature</li> </ul> <p>During the registration and certificate generation process it is essential that the EIDI-V certificate issued relates ONLY to the device from which the request has been generated. This may be achieved by a direct, in-person generation by the Registration Authority of the certificate request on the requesting device or by confirmation utilising certificate signature checks to ensure the appropriate chain of control from request, to generation to installation of the certificate.</p>		
<b>FIELDS</b>	<b>CONTENT</b>	<b>DEMARCATON</b>
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha1RSA	Fixed
Issuer		
Common Name (CN)	Issuing Certification Authority Name	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	Company Name	Fixed
Country (C)	Issuing Certification Authority Jurisdiction	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Commercial Subject Name or First Name - Last Name	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable

Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Accounting Services (OeIDI)/Third Party Services (art. 9 OeIDI)	Fixed
Organisation (O)	Organisation Name	CH Variable
Locality (L)	Not Stipulated	CH Variable
State/Province (SP)	Not Stipulated	CH Variable
Country (C)	Not Stipulated	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
<b>Extensions</b>		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature	Fixed
Key Usage	Non Repudiation	Fixed
Private Key Usage	Validity of Private Key < Cert	CH Variable
Certificate Policies	<a href="http://www.quovadisglobal.com/cps">http://www.quovadisglobal.com/cps</a>	Fixed
Policy Qualifier User Notice	Gestuetzt auf Art. 2 Abs. 2 EIDI-V; en vertu de l'art 2 al. 2 OeIDI; visto l'art. 2 cpv. 2 OeIDI; based on art. 2 para. 2 OeIDI; SR 641.201.1 / RS 641.201.1 Schweiz/Suisse/Svizzera/Switzerland	Fixed
Authority Information Access	<a href="http://ocsp.quovadisglobal.com">http://ocsp.quovadisglobal.com</a>	Fixed
Subject Alternative Name	Commercial register identification number (ASN-1 printableString coded)	CH Variable
Subject Alternative Name	Email Address (RFC 822 Name)	CH Variable
Issuer Alternative Name	O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA	Fixed
CRL Distribution	<a href="http://crl.quovadisglobal.com/qvtsagca.crl">http://crl.quovadisglobal.com/qvtsagca.crl</a>	Fixed
Thumbprint Algorithm	sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	<a href="http://www.quovadisglobal.com/cps">www.quovadisglobal.com/cps</a>	Fixed

10.1.6. Special Purpose Certificates

<b>INITIAL REGISTRATION</b>	
<ul style="list-style-type: none"> <li>Issued by QuoVadis Issuing Certification Authority.</li> <li>Registration performed by a QuoVadis Registration Authority.</li> </ul>	
<b>DESCRIPTION</b>	
Special Purpose Digital Certificates include certificates issued primarily for one or more of the Extended Key Usages as shown below. These certificates may be issued to natural persons, devices or organisations.	
<b>REGISTRATION PROCESS</b>	
An application form for a Special Purpose Digital Certificates is submitted, defining the contents of the fields required to be completed. For	
<ul style="list-style-type: none"> <li>Natural person: a copy of an official photo ID document with signature or the confirmation of a notary or other accredited third party regarding the correctness and the completeness of the data is required. Where applicable, the affiliation of a person named in a certificate to a stated organization must be confirmed by an authorized member of that organization, which may be verified by phone.</li> <li>E-mail address: the correctness is verified by an access test or by confirmation from the organization with which the individual is associated.</li> <li>Organizations are verified by presentation of a copy of a document, which proves the existence of the organization, or by verification from an official register.</li> <li>Device details: confirmation of device serial number or other unique identifying mark sought by the applicant.</li> </ul>	
<b>DIGITAL CERTIFICATE GENERATION</b>	
Certificates may be generated at the CA based on information received and verified during the application process, or based on submission of an electronic request in a prescribed format received from a party obligated by contract to verify such information.	
Certificates may be delivered by email, download or on media, subject to sufficient controls in place regarding the delivery mechanism to ensure secure delivery.	
<b>FIELDS</b>	<b>CONTENT</b>
Version	Version 3
Serial Number	Unique Number System Generated
Signature Algorithm	Sha1RSA
<b>Issuer</b>	
Common Name (CN)	Issuing Certification Authority Name
Organisational Unit (OU)	Issuing Certification Authority
Organisation (O)	Company Name
Country (C)	Issuing Certification Authority Jurisdiction
Valid From	MM/DD/YYYY HH:MM A.M/P.M
Valid To	MM/DD/YYYY HH:MM A.M/P.M
<b>Subject</b>	
Email Address (E)	<a href="mailto:aaa@bbb.xx.yy">aaa@bbb.xx.yy</a> or <a href="mailto:aaa@bbb.com">aaa@bbb.com</a>
Common Name (CN)	First Name – Middle Initial (Optional) - Last Name
Organisational Unit (OU)	Standard Commercial
Organisational Unit (OU)	Authentication
	-or-
	Application Development
	-or-
	Client /Certificate Dependent
Organisational Unit (OU)	Not Stipulated
Organisation (O)	QuoVadis Trust Services
Country/Locality	Variable Data
Subject Public Key Information	RSA (1024/2048 bit) / System Generated
<b>Extensions</b>	
Authority Key Identifier	Directory Attributes Certificate Issuer
Subject Key Identifier	ID of Certificate Holder key
Key Usage	Digital Signature (Optional)
Key Usage	Non Repudiation (Optional)
Key Usage	Key Encipherment (Optional)
Key Usage	Data Encipherment (Optional)

Key Usage	Key Agreement (Optional)
Extended Key Usage	Server Authentication
Extended Key Usage	Client Authentication
Extended Key Usage	Code Signing
Extended Key Usage	IPSEC End Entity
Extended Key Usage	IPSEC Tunnel
Extended Key Usage	IPSEC User
Extended Key Usage	Timestamp
Extended Key Usage	OCSP Server
Extended Key Usage	Individual Code Signing
Extended Key Usage	Commercial Code Signing
Extended Key Usage	Trust Signature
Extended Key Usage	Microsoft Server Gated Cryptography
Extended Key Usage	Encrypted File System
Extended Key Usage	EFS Recovery
Extended Key Usage	Netscape Server Gated Cryptography
Extended Key Usage	Smartcard Logon
Certificate Policies	<a href="http://www.quovadis.bm/pn">http://www.quovadis.bm/pn</a>
Authority Information Access	<a href="https://www.ocsp.quovadisoffshore.com">https://www.ocsp.quovadisoffshore.com</a>
Subject Alternative Name	Principle Name = Email Address
CRL Distribution	<a href="http://www.ocsp.quovadisoffshore.com/crl/CAname.crl">http://www.ocsp.quovadisoffshore.com/crl/CAname.crl</a>
Thumbprint Algorithm	Sha1
Thumbprint	System Generated
Policy Notice	<a href="http://www.quovadis.bm/policies">www.quovadis.bm/policies</a>

**10.1.7 Closed Community Certificates**

Closed Community Issuing CAs can, under contract, create Certificate Profiles to match the QuoVadis Standard Commercial Certificate for issuance to employees and affiliates.

Certificates issued by Closed Community Issuing CAs are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone certificate policy to its community issue various certificates that differ from the Standard Commercial Certificate.

QuoVadis must approve all closed community certificate policies to ensure that they do not conflict with the terms of the QuoVadis CP/CPS.

Under no circumstances can Closed Community Issuing CAs issue Qualified Certificates under the Swiss Digital Signature law.

---

## 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 PKI unless context otherwise requires:

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

**“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 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 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 Certification Authority operating within the QuoVadis PKI that defines all associated rules and indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements;

**“Certificate 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 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”** 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 subject or entity.

**“Identification”** means reliance on data to distinguish and Identify an entity or subject.

**“Individual”** means a natural person.

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

**“Issuing Certification Authority Agreement”** an agreement entered into between QuoVadis and an Issuing CA to provide Issuing CA services within the QuoVadis PKI.

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

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

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

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

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

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

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

**“PKCS”** means Public-Key Cryptography Standard.

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

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

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



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

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

**“Qualified Certificate”** A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the qualification requirements defined by the applicable legal framework of 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 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 Certification Authority to operate within the QuoVadis PKI responsible for identification and authentication of Certificate Holders.

**“Registration Authority Agreement”** an agreement entered into between an Issuing CA and a Registration Authority pursuant to which that Registration Authority is to provide its services within the QuoVadis PKI.

**“Registration Authority Certificate”** means a digital identifier issued by an Issuing CA (including QuoVadis in its capacity as an Issuing CA) in connection with the establishment of a Registration Authority within the QuoVadis PKI.

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

**“Relying Party”** means a party that acts in reliance on a Digital Certificate.

**“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 Certification Authorities.

**“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 Certification Authority Certificates.

**“Secure Signature Creation Device”** means a secure container specifically designed to carry and protect a digital certificate most commonly associated with a security rating, for example Federal Information Processing Standards (FIPS) Levels 1,2,3 etc.

**“Token”** means a Cryptographic Module consisting of a hardware object (e.g., a “smart card”), often with a memory and microchip.

**“Utility Certificate”** means a Digital Certificate issued to a Responsible Person/s to be used in the day-to-day administration of the QuoVadis PKI.

**“Validation”** means an online check, by Online Certificate Status Protocol request, or a check of the applicable Certificate Revocation List(s) (in the absence of Online Certificate Status Protocol capability) of the validity of a Digital Certificate and the validity of any Digital Certificate in that Digital Certificate's Certificate Chain for the purpose of confirming that the Digital Certificate is valid at the time of the check (i.e., it is not revoked or expired).