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: 26 February 2007

Version: 4.2

Copyright © QuoVadis 2007. All rights reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by QuoVadis.

Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement herein after referred to as the Certificate Policy & Certification Practice Statement (CPCPS), adopted by QuoVadis Limited, (QuoVadis). The QuoVadis Certificate Policy & Certification Practice Statement contains an overview of the practices and procedures that QuoVadis employs for its operation as a Digital Certification Authority. This document is not intended to create contractual relationships between QuoVadis Limited and any other person. Any person seeking to rely on Digital Certificates or participate within the QuoVadis Public Key Infrastructure must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business. This version of the Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement becomes effective is indicated on this Certificate Policy & Certification Practice Statement. The most recent effective copy of this Certificate Policy & Certification Practice Statement supersedes all previous versions. No provision is made for different versions of this Certificate Policy & Certification Practice Statement to remain in effect at the same time.

This Document covers aspects of the QuoVadis Public Key Infrastructure that relate to ALL Certification Authorities established by QuoVadis. There are a number of instances where either the legal and regulatory framework regarding the issuance of Qualified Certificates under 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
Electronic mail: policy@quovadis.bm

Version Control:

Author	*Date*	*Version*	*Comment*
QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	WebTrust Revisions
QuoVadis PMA	01 April 2004	2.07	WebTrust Revisions
QuoVadis PMA	11 November 2005	2.08	WebTrust Revisions
QuoVadis PMA	17 April 2006	4.00	Cumulative ZertES Revisions
QuoVadis PMA	14 September 2006	4.1	EIDI-V Certificate Requirements
QuoVadis PMA	26 February 2007	4.2	QuoVadis Root CA 3 added

Table of Contents

1. INTRODUCTION 1
1.1. Overview 1
1.2. Document Name And Identification 2
1.3. Public Key Infrastructure Participants 2
1.4. Certificate Usage 8
1.5. Certificate Validity Period 8
1.6. Policy Administration 8
1.7. Definitions and Acronyms 10
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 10
2.1. Repositories 10
2.2. Publication of Certificate Information 10
2.3. Time or Frequency of Publication 10
2.4. Access Controls on Repositories 10
3. IDENTIFICATION AND AUTHENTICATION 10
3.1. Naming 11
3.2. Initial Identity Validation 12
3.3. Identification And Authentication For Renewal Requests 13
3.4. Identification and Authentication For Revocation Requests 14
4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS 14
4.1. Certificate Application 14
4.2. Certificate Application Processing 15
4.3. Certificate Issuance 15
4.4. Certificate Acceptance 16
4.5. Key Pair And Certificate Usage 17
4.6. Certificate Re-Key 17
4.7. Certificate Renewal 18
4.8. Certificate Modification 18
4.9. Certificate Revocation And Suspension 18
4.10. Certificate Status Services 21
4.11. End Of Subscription 21
4.12. Key Escrow And Recovery 21
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 21
5.1. Physical Controls 21
5.2. Procedural Controls 22
5.3. Personnel Controls 23
5.4. Audit Logging Procedures 24
5.5. Records Archival 25
5.6. Key Changeover 26
5.7. Compromise And Disaster Recovery 26
5.8. Certification Authority And/Or Registration Authority Termination 26
6. TECHNICAL SECURITY CONTROLS 27
6.1. Key Pair Generation And Installation 27
6.2. Private Key Protection And Cryptographic Module Engineering Controls 28
6.3. Other Aspects Of Key Pair Management 30
6.4. Activation Data 30
6.5. Computer Security Controls 31
6.6. Life Cycle Technical Controls 31
6.7. Time-Stamping 32
7. CERTIFICATE, CRL, AND OCSP PROFILES 32
7.1. Certificate Profile 32
7.2. Certificate Revocation List Profile 33
7.3. Online Certificate Status Protocol Profile 33
7.4. Lightweight Directory Access Protocol Profile 33
7.5. Root And Issuing Certification Authority Profiles And Certificate Fields 35
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 43
8.1. Frequency, Circumstance And Standards Of Assessment 43
8.2. Identity And Qualifications Of Assessor 43

8.3. Assessor's Relationship To Assessed Entity....44
8.4. Topics Covered By Assessment....44
8.5. Actions Taken As A Result Of Deficiency....44
8.6. Publication Of Audit Results....45
9. OTHER BUSINESS AND LEGAL MATTERS....45
9.1. Fees....45
9.2. Financial Responsibilities....45
9.3. Confidentiality Of Business Information....46
9.4. Responsibility To Protect Confidential Information....46
9.5. Intellectual Property Rights....48
9.6. Representations And Warranties....48
9.7. Disclaimers Of Warranties....50
9.8. Liabilities....50
9.9. Indemnities....52
9.10. Term And Termination....52
9.11. Individual Notices And Communications With Participants....53
9.12. Amendments....53
9.13. Dispute Resolution Provisions....53
9.14. Governing Law....53
9.15. Compliance With Applicable Law....54
9.16. Miscellaneous Provisions....54
9.17. Other Provisions....54
10. APPENDIX A....55
10.1. Digital Certificate Profiles....55
10.1.1. Standard Test Certificate....56
10.1.2 Standard Personal Certificate....58
10.1.3 Qualified Personal Certificate....60
10.1.4. Standard Commercial Certificate....62
10.1.5. Qualified Commercial Certificate....64
10.1.5.1 Commercial - EIDI-V Certificates....66
10.1.6. Device Digital Certificates....68
10.1.7 Closed Community Certificates....69
11 APPENDIX B....70
11.1 Definitions and Interpretation....70

1. INTRODUCTION

1.1. Overview

The QuoVadis Certificate Policy & Certification Practice Statement sets out the policies, processes and procedures followed in the generation, issue, use and management of Digital Certificates and the roles, responsibilities and relationships of participants within the QuoVadis Public Key Infrastructure.

The Certificate Policy & Certification Practice Statement outlines the trustworthiness and integrity of the QuoVadis Root Certification Authority's operations. A fundamental concept underpinning the operation of the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure.

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 synthesizes 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 Public Key Infrastructure's operational hierarchy by binding Participants to contractual agreements. This Certificate Policy & Certification Practice Statement is not intended to create a contractual relationship between QuoVadis and any Participant in the QuoVadis Public Key Infrastructure. This Certificate Policy & Certification Practice Statement merely provides a general overview of the QuoVadis Public Key Infrastructure including Digital Certificate Profiles as defined in Appendix A.

The QuoVadis Public Key Infrastructure 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 Public Key Infrastructure must do so pursuant to definitive contractual documentation.

This Certificate Policy & Certification Practice Statement undergoes a regular review process and is subject to amendment as prescribed by the QuoVadis Policy Management Authority.

The structure of this Certificate Policy & Certification Practice Statement is based on Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, but does not seek to adhere or follow it exactly.

Any and all references to a Certificate Policy within every aspect the QuoVadis Public Key Infrastructure refers to policies contained in the current and in-force Certificate Policy & Certification Practice Statement.

1.2. Document Name And Identification

The Object Identifier (OID) arcs that QuoVadis uses to identify the Certificate Policies under which it issues certificates pursuant to this Certificate Policy & Certification Practice Statement are as follows:

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 Certificate Policy & Certification Practice Statement 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.

1.3. Public Key Infrastructure Participants

The QuoVadis Certificate Policy & Certification Practice Statement outlines the roles and responsibilities of all parties involved in the generation and use of Digital Certificates and the operation of all QuoVadis approved:

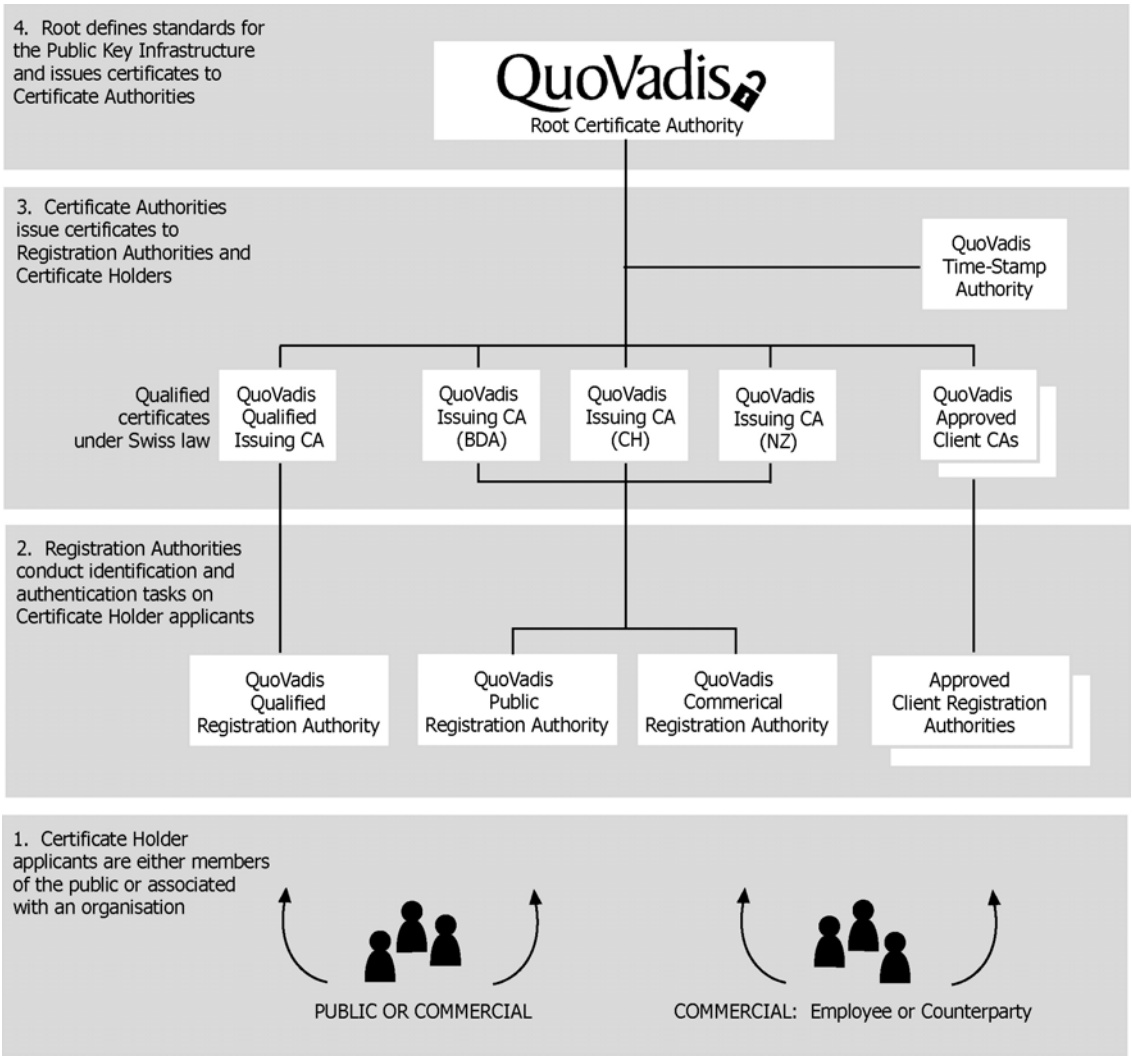
- Issuing Certification Authority services.
- Registration Authority services.

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 Public Key Infrastructure. The QuoVadis Root Certification Authority digitally creates, signs and issues Issuing Certification Authority Certificates with one of the Root Certificates identified above. Issuing Certificates are only issued to Approved Issuing Certification Authorities. An Approved Issuing Certification Authority utilises its Issuing CA Certificate to create, sign and issue Digital Certificates. Approved Registration Authorities act as the interface between Issuing Certification Authorities 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 Certification Authority 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 Public Key Infrastructure please refer to the Key Terms and Definitions in Appendix B

The diagram below illustrates the components of the QuoVadis Public Key Infrastructure:



QuoVadis provides identification and authentication services for Digital Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this Certificate Policy & Certification Practice Statement 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 Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement 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 Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement:

- 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 Certificate Policy & Certification Practice Statement, of describing the uniformity and efficiency of practices throughout the QuoVadis Public Key Infrastructure.

In keeping with their primary purpose, the practices described in this Certificate Policy & Certification Practice Statement:

- 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, contracts signing applications, custom e-Commerce applications etc.

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

1.3.1. Root Certification Authority

The QuoVadis Public Key Infrastructure 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 Certification Authority Certificates and Time Stamping Authority Certificates in accordance with this QuoVadis Certificate Policy & Certification Practice Statement and related operational documents.

1.3.2. QuoVadis And The Root Certificate Object Identifier

The Private Enterprise Object Identifier 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 for certificates issued under the QuoVadis Root CA 3 Certificate is 1.3.6.1.4.1.8024.0.3.

1.3.3. QuoVadis Obligations

QuoVadis is obligated to operate the QuoVadis Root Certification Authority, QuoVadis Issuing Certification Authority and QuoVadis Registration Authorities in accordance with this QuoVadis Certificate Policy & Certification Practice Statement and other relevant operational policies and procedures with respect to the issuance and management of Digital Certificates.

1.3.4. Issuing Certification Authority Obligations

Within the QuoVadis Public Key Infrastructure all Issuing Certification Authorities 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 Certification Authorities, 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 Certification Authority has relied on a third party Registration Authority to perform Digital Certificate Holder Identification and Authentication the

Issuing Certification Authority bears all responsibility and liability for the Identification and Authentication of its Digital Certificate Holders.

Notwithstanding the foregoing, Issuing Certification Authorities 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 QuoVadis Certificate Policy & Certification Practice Statement. Issuing Certification Authorities are required to ensure that all aspects of the services they offer and perform within the QuoVadis Public Key Infrastructure are in compliance at all times with this QuoVadis Certificate Policy & Certification Practice Statement.

Without limitation to the generality of the foregoing, Issuing Certification Authorities 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 QuoVadis Certificate Policy & Certification Practice Statement.
- They comply at all times with all compliance audit requirements.
- They follow a privacy policy in accordance with this QuoVadis Certificate Policy & Certification Practice Statement and applicable Issuing Certification Authority Agreement.

1.3.5. Issuing Certification Authorities

Issuing Certification Authorities are Organisations authorised by QuoVadis to participate within the QuoVadis Public Key Infrastructure to create, issue, sign, revoke and otherwise manage Digital Certificates in accordance with their respective Issuing Certification Authority Agreement and this Certificate Policy & Certification Practice Statement. Generally, Issuing Certification Authorities will be authorised to issue and manage all types of Digital Certificates supported by this QuoVadis Certificate Policy & Certification Practice Statement.

> 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 Public Key Infrastructure, in the capacity of an Issuing Certification Authority, 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 Certification Authorities. Organisations wishing to act as Issuing Certification Authorities will be required to enter into and act in accordance with an Issuing Certification Authority Agreement and this Certificate Policy & Certification Practice Statement. Without limitation to the generality of the foregoing, Issuing Certification Authorities are required to act in accordance with and to be bound by the terms of this QuoVadis Certificate Policy & Certification Practice Statement. An Issuing Certification Authority may, but shall not be obliged to, detail its specific practices and other requirements in a Certificate Policy adopted by it following approval by the QuoVadis Policy Management Authority. QuoVadis operates the QuoVadis Root Certification Authority and QuoVadis Issuing Certification Authority in accordance with this Certificate Policy & Certification Practice Statement. Notwithstanding that the Issuing Certification Authority may delegate certain functions to a QuoVadis Registration Authority; the QuoVadis Issuing Certification Authority shall retain all responsibility for the management of Digital Certificates issued by it.

1.3.6. Registration Authority Obligations

Issuing Certification Authorities 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 QuoVadis Certificate Policy & Certification Practice Statement. All QuoVadis Registration Authorities are required to fulfil their functions and obligations in accordance with this QuoVadis Certificate Policy & Certification Practice Statement and a Registration Authority Agreement to be entered into between the QuoVadis Registration Authority and the relevant Issuing Certification Authority.

QuoVadis Registration Authorities discharge their obligations in accordance with the practices outlined in overview in this Certificate Policy & Certification Practice Statement and applicable Registration Authority Agreement.

Registration Authorities must perform certain functions in accordance with this Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements.
- Follow a privacy policy in accordance with this QuoVadis Certificate Policy & Certification Practice Statement and applicable QuoVadis Registration Authority Agreement.

1.3.7. Certificate Holders

1.3.7.1. Obligations And Responsibilities

Digital Certificate Holders are required to act in accordance with this Certificate Policy & Certification Practice Statement 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 to 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.
- Review the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing Certification Authority, Registration Authority, or QuoVadis immediately in the event that the Digital Certificate contains any inaccuracies.
- Where Key Pairs are generated by an Applicant Digital Certificate Holder, the Applicant must promptly review, verify and accept or reject the information contained in the Digital Certificate signed by the Issuing Certification Authority.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized 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 Digital Certificate Holder's Public Key.
- Immediately notify the Issuing Certification Authority, Registration Authority or QuoVadis in the event that their Private Key is compromised, or has reason to believe or suspects 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 QuoVadis or the QuoVadis Public Key Infrastructure.
- 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 to, 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 Public Key Infrastructure has been compromised.

1.3.7.2. 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 Certificate Policy & Certification Practice Statement. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

1.3.8. 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 QuoVadis Certificate Policy & Certification Practice Statement.

1.3.8.1. Obligations and Responsibilities

Authorised Relying parties are required to act in accordance with this Certificate Policy & Certification Practice Statement and 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 Public Key Infrastructure.

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.

1.3.8.2. 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 Certificate Policy & Certification Practice Statement. For the purposes of this Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement ;
- 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 or otherwise in accordance with the provisions of this QuoVadis Certificate Policy & Certification Practice Statement ;
- 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.

1.3.8.3. 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 Certificate Policy & Certification Practice Statement. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers.

1.3.8.4. Assumptions About A Certificate Holder

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

1.3.8.5. 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, as well as the contents of this Certificate Policy & Certification Practice Statement and the current set of revoked Digital Certificates published by QuoVadis (i.e. certificates have pointers to URLs where QuoVadis publishes status information, including Certificate Revocation Lists (CRLs)).

1.3.9. Other Participants

Other Participants in the QuoVadis Public Key Infrastructure are required to act in accordance with this Certificate Policy & Certification Practice Statement and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant QuoVadis documentation.

1.4. Certificate Usage

At all times utilise its Digital Certificate in accordance with this QuoVadis Certificate Policy & Certification Practice Statement 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 QuoVadis Certificate Policy & Certification Practice Statement 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 QuoVadis Certificate Policy & Certification Practice Statement or expressly set out in the Digital Certificate.

Any person participating within the QuoVadis Public Key Infrastructure irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this QuoVadis Certificate Policy & Certification Practice Statement 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 Public Key Infrastructure (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

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.

or (iii) in connection with fraud, pornography, obscenity, hate, defamation or harassment.

No reliance may be placed on Digital Certificates and Digital Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use (ii) in breach of this QuoVadis Certificate Policy & Certification Practice Statement or the relevant User 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. Certificate Validity Period

The validity period of Digital Certificate Holder Certificates will be dependent on the class of Digital Certificate in question more fully disclosed in Section 10 of this Certification Practise Statement.

1.6. Policy Administration

1.6.1. Organisation Administering the Certificate Policy & Certification Practice Statement

QuoVadis operates the Policy Management Authority that is responsible for setting Certificate Policy & Certification Practice Statement and Certificate Profile direction for the overall public key infrastructure.

1.6.2. Certificate Policy & Certification Practice Statement Applicability

This QuoVadis Certificate Policy & Certification Practice Statement is applicable to all Digital Certificates issued by the QuoVadis Root Certification Authority and by Issuing Certification Authorities. Digital Certificates issued under this QuoVadis Certificate Policy & Certification Practice Statement are intended to support secure electronic commerce and the secure exchange of information by electronic means.

1.6.3. Certificate Policy & Certification Practice Statement Revisions

The QuoVadis Policy Management Authority is the responsible authority for changes to this Certificate Policy & Certification Practice Statement. There are two possible types of policy change:

- the issue of a new Certificate Policy & Certification Practice Statement ; or
- a change to or alteration of a policy stated in an existing Certificate Policy & Certification Practice Statement.

If an existing Certificate Policy & Certification Practice Statement requires re-issue, the change process employed is the same as for 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 of the Certificate Policy & Certification Practice Statement QuoVadis may, at its sole discretion, assign a new object identifier to the modified Certificate Policy & Certification Practice Statement.

1.6.3.1. Revisions Without Notification

The only changes that may be made to this QuoVadis Certificate Policy & Certification Practice Statement without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the Policy Management Authority, materially impact any participants within the QuoVadis Public Key Infrastructure.

1.6.3.2. Revisions With Notification

In this paragraph "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.

Any change that increases the level of trust that can be placed in Digital Certificates issued under this QuoVadis Certificate Policy & Certification Practice Statement or under policies that make reference to this QuoVadis Certificate Policy & Certification Practice Statement requires thirty (30) days prior notice.

Any change that decreases the level of trust that can be placed in Digital Certificates issued under this QuoVadis Certificate Policy & Certification Practice Statement or under policies that make reference to this QuoVadis Certificate Policy & Certification Practice Statement requires forty five (45) days prior notice. The QuoVadis Certificate Policy & Certification Practice Statement applicable to any Digital Certificate supported by this QuoVadis Certificate Policy & Certification Practice Statement shall be the QuoVadis Certificate Policy & Certification Practice Statement currently in effect; no provision is made for different versions of this QuoVadis Certificate Policy & Certification Practice Statement to remain in effect at the same time.

The QuoVadis Policy Management Authority has authority to evaluate all changes and determine whether prior notification is required and whether the QuoVadis Certificate Policy & Certification Practice Statement Object Identifier should be changed.

1.6.4. Certificate Policy & Certification Practice Statement Publication and Notification

New or amended Certificate Policy & Certification Practice Statements are published on the web site www.quovadis.bm/policies. Issuing Certification Authorities are notified of changes to the Certificate Policy & Certification Practice Statement as and when they are approved.

1.6.5. Contact Person

This Certificate Policy & Certification Practice Statement is administered by the Policy Management Authority. Enquiries or other communications about this Certificate Policy & Certification Practice Statement 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
Electronic mail: policy@quovadis.bm

1.6.6. Person Determining the Certificate Policy & Certification Practice Statement Suitability

The QuoVadis Policy Management Authority determines the suitability of the Certificate Policy & Certification Practice Statement.

1.6.7. Certificate Policy & Certification Practice Statement Approval Procedures

This QuoVadis Certificate Policy & Certification Practice Statement is regularly reviewed and approved by the QuoVadis Policy Management Authority. Notice of proposed changes are recorded in the change log at the beginning of this QuoVadis Certificate Policy & Certification Practice Statement until they are approved, at which time the approved change will be recorded there permanently.

1.6.8. Publication of Certificate Policy & Certification Practice Statement

This Certificate Policy & Certification Practice Statement is published electronically in PDF format at www.quovadis.bm

1.6.9. Frequency of Publication

Newly approved versions of this Certificate Policy & Certification Practice Statement, User Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those agreements.

1.6.10. Access Control

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

1.7. 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 Public Key Infrastructure.

The QuoVadis Root Certification Authority and chained Issuing Certification Authorities maintain in a Repository a list of all Digital Certificates issued and all Revoked Digital Certificates.

2.2. Publication of Certificate Information

The QuoVadis Root Certification Authority and chained Issuing Certification Authorities 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 Section 10 of this Certificate Policy & Certification Practice Statement.

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 Certification Authorities 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 Authority's. 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 Authentications 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 Certification Authority applicants. Different naming conventions may be used in different policy domains.

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 includes the following fields:

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

The Common Name may contain the applicant's first and last name (surname). The Common Name, the Organisation 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 subscriber'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 and 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 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 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 Certification Authority 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 Certificate Policy & Certification Practice Statement and the Digital Certificate Profiles detailed in Appendix A.

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 and verify that the name is not already listed in the QuoVadis X.500 Directory.

The Subject Name of each Digital Certificate issued by a Issuing Certification Authority shall be unique within each class of Digital Certificate issued by that Issuing Certification Authority and shall conform to all applicable X.500 standards for the uniqueness of names. The Issuing Certification Authority may, if necessary, insert additional numbers or letters to the Digital Certificate subject's common name 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 Certification Authorities are not obligated to seek evidence of trademark usage by any Organisation.

3.2. Initial Identity Validation

Identity Validation is in compliance with this Certificate Policy & Certification Practice Statement and the Digital Certificate Profiles detailed in Appendix A.

3.2.1. Method To Prove Possession Of Private Key

Issuing Certification Authorities 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 Digital Certificate application. The Issuing Certification Authority shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol.

Where Key Pairs are generated by an Applicant, the relevant Issuing Certification Authority and/or Registration Authority must satisfy themselves that the Applicant does in fact possess the Private Key that correspond to the Public Key received from the Applicant. This may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the Applicant.

The relevant Issuing Certification Authority and/or Registration Authority also take reasonable steps to ensure the Applicant is the true owner of the Key Pairs. Reasonable steps might typically consist of:

- the relevant Issuing Certification Authority and/or Registration Authority checking and arranging for any other Issuing Certification Authority and/or Registration Authority within the policy domain to check their records to ensure the Public Keys are not already listed against any current operational or revoked Digital Certificates; and
- if deemed appropriate, obtaining a statutory declaration from the Applicant that they are the true owner of the Key Pairs.

If any doubt exists, the relevant Issuing Certification Authority and/or Registration Authority should not perform certification of the Key.

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 issuing certificates to 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 Organisational Unit field of any Digital Certificates issued under its name, or routinely does business under an alternative Organisational Unit identifier 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 Certification Authority or Registration Authority has a separate and pre existing commercial relationship with the Organisation under review, the Issuing Certification Authority 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 Certification Authority 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 and other documentation.

3.2.4. Non-Verified Certificate Holder Information

The QuoVadis Issuing Certification Authority may accept any form of Non-Verified Holder Information for the Issue of Class 1 Digital Certificates.

An Issuing Certification Authority within the QuoVadis Public Key Infrastructure 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 a Digital Certificate Holder's Name is associated with an Organisational Name to indicate the Digital Certificate Holder's status as a Counterparty, Employee or specifies an Authorisation level to act on behalf of an Organisation the Registration Authority will validate Applicant Digital Certificate Holders 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 Public Key Infrastructure operates in accordance with open standards under the x.509 criteria and as such Digital Certificates issued by the QuoVadis Issuing Certification Authority are fully interoperable with Digital Certificates issued by other Issuing Certification Authorities. 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 Certification Authorities, which may be enterprise Certification Authorities operated by QuoVadis' customers. Otherwise, QuoVadis Certification Authorities and subordinate Certification Authorities are not cross certified with any other Digital 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 rekey 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 Issuing Certification Authority can revoke a Digital Certificate it has issued by an authorised individual acting under the authority of the Policy Management Authority 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 Issuing Certification Authority staff revokes the Digital Certificate/s in question.

3.4.3. Certificate Holder

A Digital Certificate Holder may request that their Digital Certificate be revoked by:

- Applying in person to the Registration Authority, Issuing Certification Authority 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.

- Send a digitally signed email message to the Issuing Registration Authority, Issuing Certification Authority or QuoVadis requesting that their Digital Certificate is revoked.
- Telephonically communication a pre-existing shared secret associated with the Digital 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 Certification Authority must be completed by Applicants, which includes all registration information as described by this QuoVadis Certificate Policy & Certification Practice Statement (including, without limitation, that information set out in Appendix B) and the relevant User 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 Certification Authority in its discretion.

4.1.2. Enrolment Process And Responsibilities

Certain information concerning applications for Digital Certificates is set out in this QuoVadis Certificate Policy & Certification Practice Statement. However, the issue of Digital Certificates by Issuing Certification Authorities will be pursuant to forms and documentation required by that Issuing Certification Authority. 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 Certificate Policy & Certification Practice Statement, and (iv) the Issuing Certification Authority shall enter into contractual relations for the use of that Digital Certificate and the QuoVadis Public Key Infrastructure. Individuals and Organisations may generate a Digital Certificate application.

Each Issuing Certification Authority will adopt their own application forms and procedures that 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 Certification Authority and the Holder or imposed upon that Holder through terms and conditions binding upon him. All agreements concerning the use of, or reliance upon, Digital Certificates issued within the QuoVadis Public Key Infrastructure must incorporate by reference the requirements of this QuoVadis Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement 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 and Issuing Certification Authorities operating within the QuoVadis Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement.

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 Certification Authority, 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 Certification Authority.

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 Certification Authority, the nominating Issuing Certification Authority a 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 Officers Certificate

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

4.3.1.5. Certificate Holder Certificates

Upon accepting the terms and conditions of the User Agreement or other relevant agreement by the Applying Digital Certificate Holder, the successful completion of the application process and final approval of the application by the Issuing Certification Authority, the Issuing Certification Authority 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 and Registration Authorities within the QuoVadis Public Key Infrastructure may choose to notify Applicant Digital Certificate Holders of Digital Certificate Issuance.

4.4. Certificate Acceptance

Digital Certificate acceptance is governed by and should comply with the practices described in and any requirements imposed by the QuoVadis Certificate Policy & Certification Practice Statement.

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 Certificate Policy & Certification Practice Statement sets out what constitutes acceptance of a Digital Certificate. An Applicant that accepts a Digital Certificate warrants to the relevant Issuing Certification Authority 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 Certificate Policy & Certification Practice Statement 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 Certification Authority operating within the QuoVadis Public Key Infrastructure, the Digital Certificate Holder expressly agrees with QuoVadis and to all 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 Digital Certificate Holder that:

- No unauthorised person has ever had access to the Digital Certificate Holder's private key;
- All representations made by the Digital 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 Digital Certificate Holder had knowledge or notice of such information, and does not promptly notify QuoVadis of any material inaccuracies in such information;
- The Digital Certificate is being used exclusively for authorised and legal purposes, consistent with this Certificate Policy & Certification Practice Statement.

4.4.1. Notice Of Acceptance

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

BY ACCEPTING A DIGITAL CERTIFICATE, THE DIGITAL CERTIFICATE HOLDER 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 DIGITAL CERTIFICATE HOLDER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE DIGITAL CERTIFICATE HOLDER); (II) FAILURE BY THE DIGITAL 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 DIGITAL CERTIFICATE HOLDER'S 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 THE INTELLECTUAL PROPERTY RIGHTS OF QUOVADIS OR A THIRD PARTY.

4.4.2. Conduct Constituting Certificate Acceptance

The following constitutes acceptance of a Digital Certificate within the QuoVadis Public Key Infrastructure:

- Downloading, installing or otherwise taking delivery of a Digital Certificate.

4.4.3. Publication Of The Certificate By The Certification Authority

All Digital Certificates issued within the QuoVadis Public Key Infrastructure are made available in public repositories except where Digital Certificate Holder's have requested that the Digital Certificate not be published.

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

Issuing and Registration Authorities within the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure a Digital Certificate Holder may only use the Public and corresponding Private Key in a Digital Certificate for its lawful and indented use when the Digital Certificate Holder has accepted the User Agreement. The Digital Certificate Holder Accepts the User 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 Public Key Infrastructure agrees to and accepts the Relying Party Agreement (www.quovadis.bm/policies) by querying the existence or validity of; or by seeking to place or by placing reliance upon on 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 asses:

- The appropriateness of the use of the Digital Certificate for any given purpose and that the use is not prohibited by this Certificate Policy & Certification Practice Statement.
- 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 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 is performed in accordance with this Certificate Policy & Certification Practice Statement.

4.6.1. Circumstance For Certificate Re-Key

Digital Certificates may be renewed upon request.

4.6.2. Who May Request Re-Key

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

4.6.3. 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 Certificate Policy & Certification Practice Statement. In order to process a Re-Key request the Digital Certificate Holder is required to confirm that the:

- 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 Digital 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.

4.6.4. Notification Of New Certificate Issuance To Certificate Holder

Issuing and Registration Authorities within the QuoVadis Public Key Infrastructure may choose to notify Digital Certificate Holders of Digital Certificate Issuance.

4.6.5. Conduct Constituting Acceptance Of A Re-Key Certificate

The following constitutes acceptance of a Digital Certificate Re-Key within the QuoVadis Public Key Infrastructure:

- Downloading, installing or otherwise taking delivery of a Digital Certificate Re-Key.

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

All Digital Certificate Re-Keys issued within the QuoVadis Public Key Infrastructure are made available in public repositories except where Digital Certificate Holder's have requested that the Digital Certificate not be published.

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

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

4.7. 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 Public Key Infrastructure does not support Renewal and the following do not apply to this Certificate Policy & Certification Practice Statement:

- 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 Digital Certification Authority.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

4.8. Certificate Modification

The QuoVadis Public Key Infrastructure does not support Digital Certificate Modification and the following do not apply to this Certificate Policy & Certification Practice Statement:

- 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:

- QuoVadis Digital 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.
- The Digital Certificate Holder has failed to meet their obligations under this QuoVadis Certificate Policy & Certification Practice Statement 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 Certification Authority determines that its Digital Certificates or the QuoVadis Public Key Infrastructure could become compromised and that revocation of Digital Certificates is in the interests of the Public Key Infrastructure, 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 Certificate Policy & Certification Practice Statement or other contractual documents.

4.9.2. Who Can Request Revocation

The following entities may request revocation of a Digital Certificate Holder Digital Certificate:

4.9.2.1. QuoVadis

QuoVadis may revoke any Digital Certificate issued within the QuoVadis Public Key infrastructure 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

Issuing Certification Authorities operating within the QuoVadis Public Key Infrastructure may revoke Digital Certificates that it has issued.

4.9.2.3. Registration Authorities

Registration Authorities operating within the QuoVadis Public Key Infrastructure may request revocation of Digital Certificates that it requested to be issued.

4.9.2.4. Certificate Holder

A Digital Certificate Holder within the QuoVadis Public Key Infrastructure may request revocation of their Digital Certificate.

4.9.3. Procedure For Revocation Request

QuoVadis will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the Issuing Certification Authority 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 Certification Authority may be required to provide a 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 Certification Authority or Registration Authority administrators 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 Certification Authority and providing adequate proof of identification in accordance with this QuoVadis Certificate Policy & Certification Practice Statement or an equivalent method.

4.9.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. Issuing Certification Authorities 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 Certification Authority 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 Certification Authority 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 Certification Authority 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 requests.

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 Certification Authority provides an on line 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.

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 Public Key Infrastructure.

4.9.14. Who Can Request Suspension

No suspension of Digital Certificates is permissible within the QuoVadis Public Key Infrastructure.

4.9.15. Procedure For Suspension Request

No suspension of Digital Certificates is permissible within the QuoVadis Public Key Infrastructure.

4.9.16. Limits On Suspension Period
No suspension of Digital Certificates is permissible within the QuoVadis Public Key Infrastructure.

4.10. Certificate Status Services
4.10.1. Operational Characteristics
The Status of Digital Certificates issued within the QuoVadis Public Key Infrastructure is published in a Certificate Revocation List www.quovadisoffshore.com/crl/issuing ca name.crl) or is made available via Online Certificate Status Protocol checking (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 Public Key Infrastructure 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 Escrow And Recovery
The QuoVadis Public Key infrastructure does not support Key Escrow.

4.12.1. Key Escrow And Recovery Policy And Practices
The QuoVadis Public Key infrastructure does not support Key Escrow.

4.12.2. Session Key Encapsulation And Recovery Policy And Practices
Not Applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
5.1. Physical Controls
QuoVadis Manage and implement appropriate physical security controls to restrict access to the hardware and software used in connection with Issuing Certification Authority operations wherever those operations physically occur.

5.1.1. Site Location and construction
The site location of QuoVadis is in a secure office environment in Bermuda. QuoVadis operates within a secure Data-Centre within the office area that meets the standards of an independent security certification body, at a highly protected level. Standards 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); 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 authorized personnel.

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.

5.1.5. Fire Prevention And Protection
The QuoVadis secure operating area provides protection against fire.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

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

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

5.1.8. Off-Site Backup

Endorsed off site storage agents are used for the storage and retention of backup software and data.
The off site storage:

- is available to authorized 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.

5.2. Procedural Controls

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

Issuing Certification Authorities 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 Certificate Policy & Certification Practice Statement and other relevant operational documents.

It is company policy that QuoVadis will not outsource any of its Public Key Infrastructure operations to other organizations.

5.2.1. Trusted Roles

In order to ensure that one person acting alone cannot circumvent the entire system, responsibilities are shared by multiple roles and individuals. Oversight may be in the form of a person who is not directly involved in issuing Digital Certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles.

5.2.2. Number Of Persons Required Per Task

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

Digital Certification Authority key-pair generation and initialisation of each of the Digital Certification Authority/ies (Root and Operational) 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 Certification Authorities will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. Issuing Certification Authorities must ensure that no single Individual may gain access to a User's Private Key if stored by the Issuing Certification Authority. At a minimum, procedural or operational mechanisms must be in place for Issuing Certification Authority Key recovery in disaster recovery situations. To best ensure the integrity of the Issuing Certification Authority equipment and operation, Issuing Certification Authorities 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 stored on an approved cryptographic smart card to identify themselves to the Digital Certificate server and Repository.

5.2.4. Roles Requiring Separation Of Duties

Operations involving Root Certificate and Issuing Certification Authority roles are segregated between M of N employees. All operations involving maintenance of Audit Logs are segregated.

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 Public Key Infrastructure or any Digital Certificate issued therein, QuoVadis shall perform relevant background checks of individuals and define tasks that the Individuals will be responsible to perform. QuoVadis shall determine 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
- Social security records

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

5.3.3. Training Requirements

QuoVadis provides its personnel with on the job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities 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 all required training materials needed to perform their job function and their duties under the job rotation program.

5.4. Audit Logging Procedures
5.4.1. Types Of Events Recorded
All events involved in the generation of the Digital 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 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 being present to perform certain tasks on the QuoVadis Digital 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.
- 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.

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 11 (eleven) years for audit trail files, and no less than 11 (eleven) years for Key and Digital Certificate information. Audit logs are stored until at least 11 (eleven) 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 Public Key Infrastructure.

Only Digital 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 Certification Authority performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing Certification Authority's premises and storage at a secure off site location.

Backup procedures apply to the QuoVadis Public Key Infrastructure and the participants therein including the QuoVadis Root Certification Authority, Issuing Certification Authorities and Registration Authorities.

5.4.6. Audit Collection System

The security audit process of each Issuing Certification Authority runs independently of the Issuing Certification Authority 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 will be carried out on all parts of the QuoVadis Public Key Infrastructure environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Issuing Certification Authority. Vulnerability assessment procedures intend to identify QuoVadis Public Key Infrastructure 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 authorized request, documentation related to and subject to the QuoVadis Document Access Policy. For each Digital Certificate, the records will address creation, issuance, use, revocation, expiration, and renewal activities. These records will include all relevant evidence in the Issuing Certification Authority'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) User 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 Certificate Policy & Certification Practice Statement; 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 11 (eleven) years.

5.5.3. Protection Of Archive

Archives shall be retained and protected against modification or destruction. Only Issuing Certification Authority 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 recognized representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval. Requests for access to archived information should be sent electronically to QuoVadis.

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements For Time-Stamping Of Records

QuoVadis supports time stamping of all of its records. All events that are recorded within 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 Digital Certification Authority program is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure to preserve their audit trails.

5.5.7. Procedures To Obtain And Verify Archive Information

Digital Certificate Holder Private Keys shall only be obtained by:

- A legitimate request from the Digital Certificate Holder where the identity of the Digital Certificate Holder is positively achieved; or
- A legitimate and lawful judicial order that complies with requirements of this Certificate Policy & Certification Practice Statement.

5.6. Key Changeover

Key changeover is not automatic. Keys expire at the same time as their associated Digital Certificates and, with the exception of the QuoVadis Root Certification Authority which issues a new Digital Certificate and new Keys to itself, all parties within the QuoVadis Public Key Infrastructure are to obtain new keys by making an application for Digital Certificate renewal to the corresponding Registration Authority and subject to any relevant contractual documentation and fees.

5.7. Compromise And Disaster Recovery

QuoVadis has a Digital Certification Authority 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 Certification Authority has 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 and that it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.

QuoVadis and each Issuing Certification Authority has in place an appropriate Key compromise plan detailing its activities in the event of a compromise of a QuoVadis Issuing Certification Authority Private Key. Such plans include procedures for:

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

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 Certification Authority 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 Certification Authority and/or the Registration Agreements.
QuoVadis and each Issuing Certification Authority specifies the procedures it will follow when terminating all or a portion of its Digital Certificate issuance and management operations. The procedures must, at a minimum:

- ensure any disruption caused by the termination of an Issuing Certification Authority is minimised;
- ensure that archived records of the Issuing Certification Authority are retained;
- ensure that prompt notification of termination is provided to Digital Certificate Holders, Authorised Relying Parties, and other relevant parties in the QuoVadis Public Key Infrastructure;
- ensure that a process for revoking all Digital Certificates issued by an Issuing Certification Authority 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 Certification Authority 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 Certification Authority.

5.8.2. Successor Issuing Certification Authority

To the extent that it is practical and reasonable the successor Issuing Certification Authority should assume the same rights, obligations and duties as the terminating Issuing Certification Authority. The successor Issuing Certification Authority 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 Certification Authority 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 User Agreement.

5.8.3. Private Key Destruction Procedures

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 unauthorized use.

Upon termination of the Issuing Certification Authority, QuoVadis personnel shall destroy the QuoVadis Digital Certification Authority private key by deleting, overwriting or physical destruction.

6. TECHNICAL SECURITY CONTROLS

The QuoVadis Digital Certification Authority private keys are protected within a hardware security module with Federal Information Processing Standard-140 level 4 capabilities. 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 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 the registration information is collected by the QuoVadis Digital Certification Authority the Digital Certificate Holders 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 Certification Authorities, 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 an FIPS approved method.

6.1.2. Private Key Delivery To Certificate Holder

Once the Digital Certificate Holder Certificate request has been signed the Certificate Holder's Digital Certificate and private key will be distributed in person or via a secure channel whereby only the Digital Certificate Holder will have access to his/her private key.

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 Certification Authority 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 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. Off line means will include Identity checking and will not inhibit proof of possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a User Agreement or other agreement. In those cases where Key Pairs are generated by the Issuing Certification Authority on behalf of the Holder, the Issuing Certification Authority 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

Public Keys of QuoVadis and each Issuing Certification Authority shall be publicly available.

6.1.5. Key Sizes

Key lengths within the QuoVadis Public Key Infrastructure are determined by Digital Certificate Profiles more fully disclosed in section 10. The QuoVadis Issuing Certification Authority uses an RSA minimum key length of 1,024 bit modulus.

6.1.6. Public Key Parameters Generation And Quality Checking

The parameters used to create Public Keys are generated by the relevant Registration Authority application, except for self-generated User keys in which case the parameters are generated by the User's client application.

The quality of Public Key parameters is automatically checked by the Registration Authority that generates the Key, except for self-generated User Keys in which case the parameters are quality checked by the Registration Authority prior to submitting a Digital Certificate request to the appropriate Issuing Certification Authority.

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 Certificate Policy & Certification Practice Statement – Digital Certificate Profiles.

Issuing Certification Authorities Private Keys are used for Digital Certificate signing and Certificate Revocation List signing. It may also be used to authenticate the Issuing Certification Authority to a Repository.

6.2. Private Key Protection And Cryptographic Module Engineering Controls

All participants in the QuoVadis Public Key Infrastructure are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this QuoVadis Certificate Policy & Certification Practice Statement. Without limitation to the generality of the foregoing, all participants in the QuoVadis Public Key Infrastructure 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 their 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 Certification Authorities 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 Certification Authorities in the QuoVadis Public Key Infrastructure is designed to provide Federal Information Processing Standard-140 Level 4 security standards in both the generation and the maintenance in all Root and Operational Digital Certification Authority 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

Subject to the requirements of sections 5.2 & 5.3 of the current and in force QuoVadis Certificate Policy & Practice statement the QuoVadis Public Key Infrastructure uses trusted multi-person control for both access control and authorisation control.

6.2.3. Private Key Escrow

Private Keys shall not be escrowed.

6.2.4. Private Key Backup

Issuing Certification Authority Private Keys are stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secure off site storage. All Issuing Certificate Authority Keys are held in a secure cryptographic device and is equally secured when it is stored outside a secure cryptographic device.

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 both encrypted and decrypted forms, 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 unauthorized 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.

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.

6.2.11. Cryptographic Module Rating

Cryptographic modules in use with the QuoVadis Public Key Infrastructure comply with industry 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.

The validity period of Digital Certificate Holder Digital Certificates will be dependent on the class of Digital Certificate in question.

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 Pubic Key Infrastructure are:

- Root CA certificate — 25 years
- All Issuing CA certificates — 10 years
- Qualified Personal Certificates (According to Swiss Digital Signature law) — 1 year
- Qualified Commercial Certificates (According to Swiss Digital Signature law) — 1 year
- 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 must be randomly and automatically generated. No activation data other than access control mechanisms is required to operate Cryptographic Modules.

A unique User Personal Identification Code may be generated by a Registration Authority during key pair creation, to protect the transport of a User's Keys and Digital Certificates to the User.

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.

6.4.2. Activation Data Protection

No activation data other than access control mechanisms is required to operate Cryptographic Modules. Personal Identification Codes may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third party interception of the Personal Identification Code. Activation Data should be memorized, not written down. Activation Data must never be shared. Activation data must not contain Digital Certificate Holders 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 Certification Authority must establish an approved System Security Policy that incorporates computer security technical requirements that are specific to that Issuing Certification Authority's operations.

The QuoVadis Issuing Certification Authority 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 Digital 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, Public Key Infrastructure 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 Public Key Infrastructure roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and Public Key Infrastructure roles, see Section 5.2
- Identification and Authentication of personnel that fulfil roles of responsibility in the QuoVadis Public Key Infrastructure, 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 Issuing Certification Authority within the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure 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 Certification Authority within the QuoVadis Public Key Infrastructure must be maintained by causing it to be shipped or delivered via controlled methods. Issuing Certification Authority equipment shall not have installed applications or component software that is not part of the Issuing Certification Authority configuration. All subsequent updates to Issuing Certification Authority 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 ratings that are specific to QuoVadis and deal with, including but not limited to:

6.6.1. System Development 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.

6.6.2. 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.

6.6.4. Network Security Controls

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

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

6.6.5. Hardware Cryptographic Module Engineering Controls

Cryptographic modules used by the QuoVadis Root Certification Authority, Issuing Certification Authorities, and Registration Authorities are certified to Internet Engineering Task Force (IETF) Standards, and are either FIPS 140-2 Level 3 or EAL 4 compliant.

6.7. Time-Stamping

The QuoVadis Time-stamping Authority uses Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement.

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 utilize the ITU-T X.509 version 3 Digital Certificate standard.

For the purposes of this QuoVadis Certificate Policy & Certification Practice Statement, Digital Certificates, other than the QuoVadis Root Certificates and Issuing Certificates, all other Digital Certificate profiles within the QuoVadis PKI are detailed in Appendix A:

7.1.1. Certificate Content
A QuoVadis Digital Certificate only certifies the information contained therein.

7.1.2. Version Numbers
Digital Certificates in the QuoVadis Public Key Infrastructure are x.509 Version 3

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

7.1.4. Algorithm Object Identifiers
No Stipulation.

7.1.5. Name Forms
See 3.1.1

7.1.6. Name Constraints
See 3.1.1

7.1.7. Certificate Policy & Certification Practice Statement Object Identifier
The Object Identifiers (OIDs) assigned to this Certificate Policy & Certification Practice Statement are 1.3.6.1.4.1.8024.0.1 and 1.3.6.1.4.1.8024.0.3.

7.1.8. Usage Of Policy Constraints Extension
No Stipulation.

7.1.9. Policy Qualifiers Syntax And Semantics
Digital Certificates issued within the QuoVadis Public Key Infrastructure contain one of the Object Identifiers for this Certificate Policy & Certification Practice Statement.

7.1.10. Processing Semantics For The Critical Certificate Policies Extension
No Stipulation.

7.2. Certificate Revocation List Profile
If utilized, Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with the Public Key Infrastructure X Digital Certificate and Certificate Revocation List Profile.

7.2.1. Version Number
Issuing Certification Authorities within the QuoVadis Public Key Infrastructure issue X.509 version 2 Certificate Revocation Lists in accordance with the PKIX Digital Certificate and Certificate Revocation List Profile.

7.2.2. Certificate Revocation List And Certificate Revocation List Entry Extensions
All User Public Key Infrastructure 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 Public Key Infrastructure.

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 Public Key Infrastructure.

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 an Lightweight Directory Access Protocol directory for the purpose of storing and making available all X.509 v 3 Digital Certificates issued under the QuoVadis Certification Authority, facilitating public access to download these Digital Certificates for Digital Certificate Holder and relying party

requirements and 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

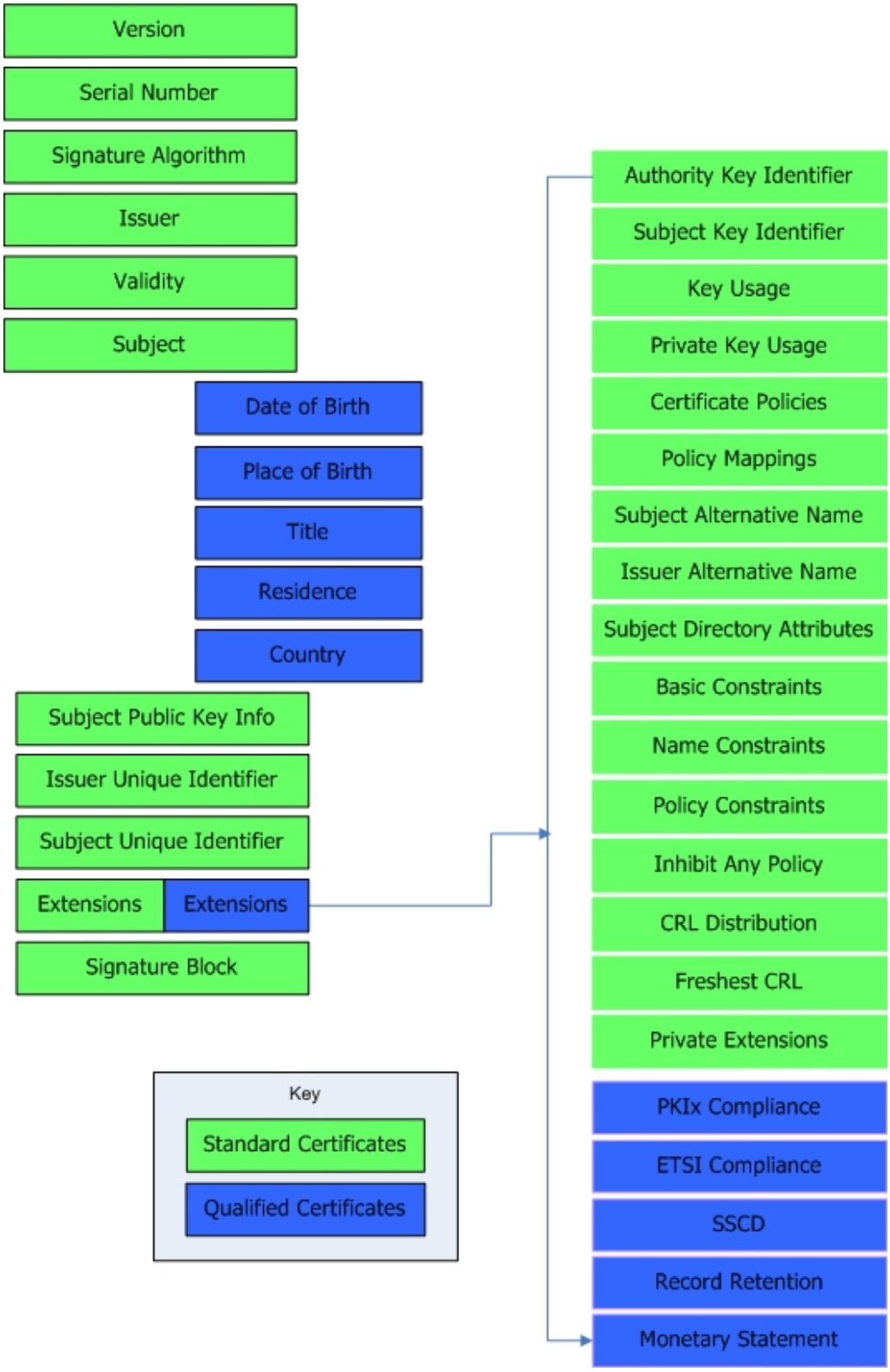
LDAP V3 in accordance with RFC-3377

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: http://www.quovadis.bm

Field	QuoVadis Issuing CA 2
	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 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 2.5.29.35: 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 2.5.29.14: 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 Signature Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA Algorithm Parameters: 05 00
Signature Block	Non-root Certificate 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

7.5.1.3. QuoVadis Issuing CA 3: 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	Certificate Extensions: 9 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None 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 [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 1.3.6.1.5.5.7.1.3: Flags = 1(Critical), Length = 18 QC Statements Qualified Digital Certificate id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) 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 & Certification Practice Statement. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPCPS Qualifier: http://www.quovadis.bm 2.5.29.15: Flags = 1(Critical), Length = 4 Key Usage

Field	QuoVadis Issuing CA 3
	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

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	Certificate Extensions: 5 2.5.29.19: Flags = 1(Critical), Length = 5 Basic Constraints Subject Type=CA Path Length Constraint=None

Field	QuoVadis Root CA 3 Profile
	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: http://www.quovadisglobal.com/cps 2.5.29.15: Flags = 0, Length = 4 Key Usage Certificate Signing, Off-line CRL Signing, CRL Signing (06) 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 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 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	

Field	QuoVadis Root CA CRL
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) symbolizes 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. Compliance audits as carried out under these provisions may substitute for audits noted in this Certificate Policy & Certification Practice Statement.

8.1.2. Issuing Certification Authorities

Issuing Certification Authorities (including QuoVadis) will undergo an audit in order to determine compliance with this QuoVadis Certificate Policy & Certification Practice Statement at least annually. These audits shall include the review of all relevant documents maintained by the Issuing Certification Authority regarding their operations within the QuoVadis Public Key Infrastructure and under this QuoVadis Certificate Policy & Certification Practice Statement, and other related operational policies and procedures.

8.1.3. Registration Authorities

Every Registration Authority within the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure. The obligations of Issuing Certification Authorities and Registration Authorities within the QuoVadis Public Key Infrastructure 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 experienced in performing information security audits, specifically having significant experience with Public Key

Infrastructure's 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 Certification Authority under audit, must not have any other relationship that would impair its 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 a Issuing Certification Authority 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 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 Certification Authority in question must submit a report to the QuoVadis Root Certification Authority detailing actions the Issuing Certification Authority will take in response to the irregularity.

Where the Issuing Certification Authority fails to take appropriate action in response to an irregularity, the QuoVadis Root Certification Authority may (i) indicate the irregularities, but allow the Issuing Certification Authority to continue operations for a limited period of time; (ii) allow the Issuing Certification Authority to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation of that Issuing Certification Authority's Issuing Certificate; (iii) limit the class of any Digital Certificates issued by the Issuing Certification Authority; or (iv) revoke the Issuing Certification Authority'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 Certification Authority'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 a Issuing Certification Authority, the principles enunciated above will be followed by the QuoVadis Root Certification Authority.

8.5.2. Registration Authorities

If irregularities are found, the QuoVadis Root Certification Authority, or if applicable the Issuing Certification Authority, 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 Certificate Policy & Certification Practice Statement. 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 Certification Authority to continue operations for a further period of time whilst the irregularities are addressed; (ii) allow the Nominating Certification Authority 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 Certification 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 Certification Authority; or (iv) terminate that Issuing Certification Authority'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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Issuing and Registration Authorities within the QuoVadis Public Key Infrastructure will make available all applicable fees upon request. Fees for Digital Certificate issuance vary widely based on 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 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 Certification Authority/ies under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. Financial Responsibilities

9.2.1. Financial Records

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.

9.2.2. 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 Public Key Infrastructure does not make any participant an agent, fiduciary, trustee, or other representative of any entity, legal or otherwise. Nothing contained in this QuoVadis Certificate Policy & Certification Practice Statement or in any corresponding User or Relying Party Agreement shall be deemed to constitute QuoVadis, QuoVadis Public Key Infrastructure 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 Public Key Infrastructure is to be construed accordingly.

9.2.3. Insurance Cover

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 Public Key Infrastructure the Root Certification Authority and all Issuing and Registration Authorities are required to demonstrate that they have the financial resources necessary to discharge their obligations under this Certificate Policy & Certification Practice Statement and any other relevant and associated documentation or agreements.

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

9.2.4. Other Assets

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

9.2.5. 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.

9.3. Confidentiality Of Business Information

9.3.1. Scope Of Confidential Information

Any personal or corporate information held by Issuing Certification Authorities 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 Certificate Policy & Certification Practice Statement.

The Issuing Certification Authority does not have access to the Private Keys of any of the entities it certifies or whose Digital Certificate requests it processes. There is no requirement to place a copy of any Private Key with any backup/recovery or escrow service. Under contract between an Issuing Certification Authority 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.

9.4. Responsibility To Protect Confidential Information

9.4.1. Privacy Of Personal Information

9.4.1.1. Privacy Plan

QuoVadis, Issuing Certification Authorities, Registration Authorities, Digital Certificate Holders, Relying Parties and all others using or accessing any personal data in connection with matters dealt with this Certificate Policy & Certification Practice Statement 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 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 and 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

The 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 Certification Authority Digital Certificate due to:

- the compromise of the Issuing Certification Authority's Private Key, in which case a disclosure may be made that the Private Key has been compromised;
- the termination of a Issuing Certification Authority within the QuoVadis Pubic 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. Certificate Policy & Certification Practice Statement

This QuoVadis Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement 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 Digital 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 to 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.

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

9.4.6.2. Release As Part Of Civil Discovery

As a general principal, 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.

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

9.4.7. Other Information Disclosure Circumstances

QuoVadis, Issuing Certification Authorities 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 Certificate Policy & Certification Practice Statement.

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 Certificate Policy & Certification Practice Statement and the Proprietary Marks are the intellectual property of QuoVadis.

QuoVadis retains exclusive title to, copyright in, and the right to license this QuoVadis Certificate Policy & Certification Practice Statement.

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 Public Key Infrastructure as outlined in this Certificate Policy & Certification Practice Statement.

9.5.3. IETF Guidelines

The use of the Public Key Infrastructure X 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

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” includes but does not limit QuoVadis to operating in compliance with:
- documented operational procedures; and
- within applicable law and regulation;
- approving the establishment of all Issuing Certification Authorities and on approval, executing a Issuing Certification Authority Agreement (save in respect of the QuoVadis Digital Certification Authority);
- maintaining this Certificate Policy & Certification Practice Statement and enforcing the practices described within it and in all relevant collateral documentation;
- publishing its Root Certification Authority Hash at www.quovadis.bm and other nominated web sites;

- Issuing Certification Authority Certificates to Issuing Certification Authorities that comply with X.509 standards and are suitable for the purpose required;
- Issuing Certification Authority 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 Certification Authority Certificates without alteration in the X.500 Directory;
- investigating any suspected compromise which may threaten the integrity of the QuoVadis Public Key Infrastructure;
- revoking Issuing Certification Authority Certificates and posting such revoked Certificates in the X.500 Directory Certificate Revocation List; and
- conducting compliance audits of Issuing Certification Authorities.

9.6.2. Certification Authority Warranties

QuoVadis 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 (b) Digital Certificates shall be revoked if QuoVadis 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 QuoVadis 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. QuoVadis makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

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

Each Issuing Certification Authority is required to ensure that warranties, if any, provided by QuoVadis in connection with this QuoVadis Certificate Policy & Certification Practice Statement to Subscribers and Authorised Relying Parties are incorporated, by reference or otherwise, in the relevant User Agreement or applicable terms and conditions. Warranties, if any, provided by QuoVadis to Subscribers 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.

9.6.3. Registration Authority Representations

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

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

9.6.4. Registration Authority Warranties

Authorised Registration Authorities operating within the QuoVadis Public Key Infrastructure 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 (b) Digital Certificates shall be revoked if QuoVadis 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.

9.6.5. Certificate Holder Representations And Warranties

Digital Certificate Holders Represent and Warrant:

- To use only the Digital Certificate Holders own valid, legal and operational Key pairs to create a Digital Signature.
- 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 Certificate Policy & Certification Practice Statement.

9.6.6. Relying Parties Representations And Warranties

Relying Parties Represent and Warrant:

- To collect enough information about a Digital Certificate and its Corresponding Holder to make an informed decision as to the extent they can rely on the Digital Certificate.
- That the relying part is solely responsible for making the decision to rely on a Digital Certificate.
- That the relying Party shall bear the legal consequences of any failure to perform Relying Party obligations under the terms of this Certificate Policy & Certification Practice Statement and Relying Party agreement.

9.6.7. Representations And Warranties Of Other Participants

Participants within the QuoVadis Public Key Infrastructure Represent and Warrant to accept and perform any and all duties and obligations as specified by this Certificate Policy & Certification Practice Statement.

9.7. Disclaimers Of Warranties

To the extent permitted by applicable law, this Certificate Policy & Certification Practice Statement, Digital Certificate Holder Agreement, Relying Party Agreement, Issuing Certification Authority Agreement, Registration Authority Agreement and any other contractual documentation applicable within the QuoVadis Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement. 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. Liabilities

9.8.1. QuoVadis Liability

QuoVadis shall be liable to Digital Certificate Holders or relying parties for direct loss arising from any breach of this Certificate Policy & Certification Practice Statement or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of See Chart 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 Certificate Policy & Certification Practice Statement, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

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 rely 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 Certificate Policy & Certification Practice Statement, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis' liability to any person for damages arising under, out of or related in any way to this QuoVadis Certificate Policy & Certification Practice Statement, User 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 Public Key Infrastructure (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the QuoVadis Public Key Infrastructure irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon the foregoing as a condition and inducement to permit that person to participate within the QuoVadis Public Key Infrastructure.

For the avoidance of doubt, QuoVadis shall bear no liability or responsibility to any person that participates in the QuoVadis Public Key Infrastructure 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 Certificate Policy & Certification Practice Statement and/or the relevant User 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 2, QuoVadis' liability for breach of its obligations pursuant to this QuoVadis Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement, 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 Certificate Policy & Certification Practice Statement becomes effective upon publication in the QuoVadis Repository. Amendments to this Certificate Policy & Certification Practice Statement become effective upon publication in the QuoVadis Repository.

9.10.2. Termination

This Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement shall survive the termination or withdrawal of a User from the QuoVadis Public Key Infrastructure with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the QuoVadis Public Key Infrastructure. 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 of QuoVadis providing any of the notices required by this QuoVadis Certificate Policy & Certification Practice Statement, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid means of providing any notice required pursuant to this QuoVadis Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement are made and approved by the QuoVadis Policy Management Authority. Amendments shall be in the form of an Amended Certificate Policy & Certification Practice Statement or a replacement Certificate Policy & Certification Practice Statement. Updated versions of this Certificate Policy & Certification Practice Statement supersede and designated or conflicting provisions of the referenced version of the Certificate Policy & Certification Practice Statement.

9.12.2. Notification Mechanism And Period

The QuoVadis Policy Management Authority reserve the right to amend this Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement is at the sole discretion of the QuoVadis Policy Management Authority.

9.12.3. Circumstances Under Which Object Identifiers Must Be Changed

Unless the QuoVadis Policy Management Authority determine otherwise the Object Identifier to this Certificate Policy & Certification Practice Statement shall not change.

9.13. Dispute Resolution Provisions

Any controversy or claim between two or more participants in the QuoVadis Public Key Infrastructure (for these purposes, QuoVadis shall be deemed a “participant” within the QuoVadis Public Key Infrastructure) arising out of or relating to this QuoVadis Certificate Policy & Certification Practice Statement shall be 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 Root Certification Authority and Issuing Certification Authority is dealt with under Bermuda Law.
- Dispute between Issuing Certification Authority and Registration Authority is dealt with under the applicable law of the Issuing Certification Authority.
- Dispute between Issuing Certification Authority and Authorised Relying Party is dealt with under the applicable law of the Issuing Certification Authority.

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 Certificate Policy & Certification Practice Statement is subject to applicable law.

9.16. Miscellaneous Provisions
Not Applicable.

9.16.1. Record Keeping
QuoVadis shall keep records material to the issue of Digital Certificates for a minimum of 10 years.

9.16.2. Entire Agreement
Not Applicable.

9.16.3. Assignment
Not Applicable.

9.16.4. Severability
Any provision of this QuoVadis Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement or affecting the validity or enforceability of such remaining provisions.

9.16.5. 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 Certificate Policy & Certification Practice Statement ; 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 Certificate Policy & Certification Practice Statement is intended to be exclusive of any other right or remedy, except as expressly provided in this QuoVadis Certificate Policy & Certification Practice Statement, 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.

9.16.6. Force Majeure
QuoVadis accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters.

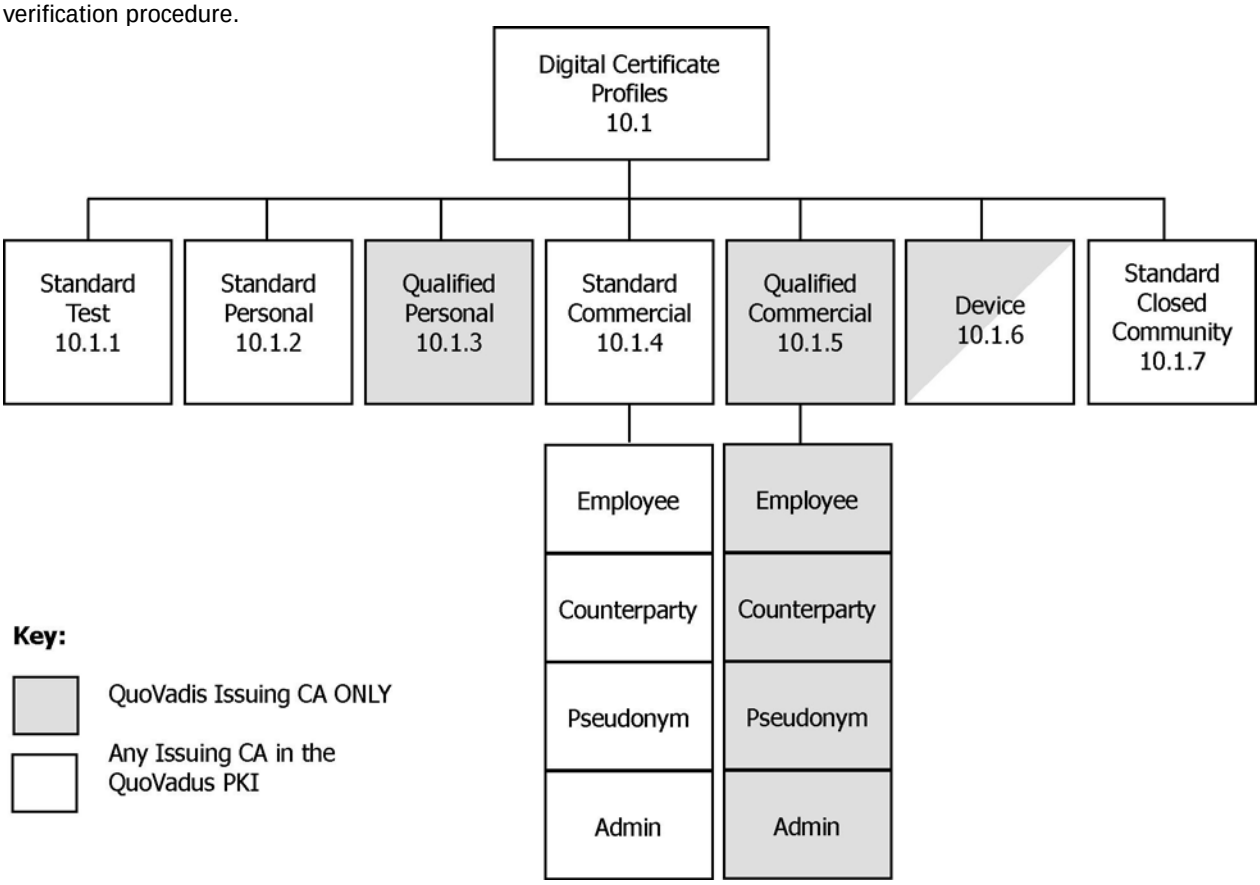
9.17. Other Provisions
No Stipulation.

10. APPENDIX A
10.1. Digital Certificate Profiles

Within the QuoVadis Public Key Infrastructure an Issuing Certification Authority can only issue Digital Certificates with approved Digital Certificate Profiles. All Digital Certificate Profiles within the QuoVadis Public Key Infrastructure 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 not described in this Certificate Policy & Certification Practice Statement 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 Certification Authority either based on policy or by IETF Standard, applicable law or regulation.

10.1.1. Standard Test Certificate

INITIAL REGISTRATION

- Issued by approved Issuing Certification Authorities in the QuoVadis Public Key Infrastructure.
- Registration performed by approved Registration Authorities in the QuoVadis Public Key Infrastructure.

IDENTIFICATION & AUTHENTICATION

There is no formal Identification & Authentication requirement for Standard Test Digital Certificates. Standard Test Digital Certificates are issued on the basis of the Applicant Digital Certificate Holder's self certification.

REGISTRATION PROCESS

Registration information may be received from an Applicant Digital Certificate Holder:

- In person, or
- By mail or electronic methods

Standard Test Digital Certificates Holders participate in the QuoVadis Public Key Infrastructure. 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.

DIGITAL CERTIFICATE GENERATION

All successful Standard Test Digital Certificate requests will be processed by the Issuing Certification Authority. Each Standard Test Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The Issuing Certification Authority will apply to the Digital Certificate request a:

- Unique serial number
- Operational Certification Authority's signature

DIGITAL CERTIFICATE DELIVERY

- Download over the Internet
- CD/Floppy Disk
- Smart Card or other secure hardware token
- E-mail

FIELDS	CONTENT	DEMARCATION
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	Sha1RSA	Fixed
Issuer		
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
Subject		
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	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
Extensions		
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	http://www.quovadis.bm/pn	Fixed
Authority Information Access	https://www.ocsp.quovadisoffshore.com	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl	Fixed
Private Extensions	Special Application	CH Variable
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.2 Standard Personal Certificate

INITIAL REGISTRATION

- Issued by the QuoVadis Issuing Certification Authority.
- Registration performed by QuoVadis Registration Authorities.

IDENTIFICATION & AUTHENTICATION

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.

REGISTRATION PROCESS

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 (*e.g.,* holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:

- in person or
- by mail or electronic methods.

The Registration and Authentication process of a Standard Personal Digital Certificate Holder's identity includes:

- the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.
- one form of government issued photographic identification is reviewed and photocopied.
- 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.

DIGITAL CERTIFICATE GENERATION

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:

- Unique serial number
- Operational Certification Authority's signature

DIGITAL CERTIFICATE DELIVERY

- Download over the Internet
- CD/Floppy Disk
- Smart Card or other secure hardware token

Certificate Pins are delivered in an out of band manner to the physical delivery method used for the Certificate.

FIELDS	CONTENT	DEMARCATION
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)	aaa@bbb.xx.yy or aaa@bbb.com	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
Extensions		
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	http://www.quovadis.bm/pn	Fixed
Authority Information Access	https://www.ocsp.quovadisoffshore.com	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.3 Qualified Personal 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.

INITIAL REGISTRATION

- Issued by QuoVadis Issuing Certification Authority.
- Registration performed by a QuoVadis Registration Authorities.

IDENTIFICATION & AUTHENTICATION

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.

REGISTRATION PROCESS

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 (*e.g.,* 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 Personal 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.
- one form of government issued photographic identification is reviewed and photocopied.
- 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.
- All information on the applicant form and all certificate fields shown in the certificate are verified as accurate.

DIGITAL CERTIFICATE GENERATION

All successful Qualified 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:

- Unique serial number
- Operational Certification Authority's signature
- Digital Certificate is generated and stored in a compliant S.S.C.D container - i.e. a secure/cryptographic smartcard or USB token.

DIGITAL CERTIFICATE DELIVERY

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.

FIELDS	CONTENT	DEMARCATION
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)	aaa@bbb.xx.yy or aaa@bbb.com	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Qualified Personal	Fixed
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Not Stipulated	CH Variable
Organisation (O)	Organisation Name	CH Variable
Date Of Birth	DD/MM/YYYY	CH Variable
Place of Birth	City	CH Variable

Title	Verified Legal Title	CH Variable
Residence	ISO Country Code – Normally Resident	CH Variable
Country	ISO Country Code – Nationality	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Non Repudiation	Fixed
Private Key Usage	Validity of Private Key < Cert	CH Variable
Certificate Policies	http://www.quovadis.bm/pn	Fixed
Authority Information Access	https://www.ocsp.quovadisoffshore.com	Fixed
Subject Alternative Name	Principal Name = Email Address	CH Variable
Issuer Alternative Name	ZertES Recognition Body KPMG Klynveld Peat Marwick Goerdeler SA	Fixed
QC Statement PKIX Compliance	1.3.6.1.5.5.7.1.3	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	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.4. Standard Commercial Certificate

INITIAL REGISTRATION

- Issued by approved Issuing Certification Authorities in the QuoVadis Public Key Infrastructure.
- Registration performed by approved Registration Authorities in the QuoVadis Public Key Infrastructure.

IDENTIFICATION & AUTHENTICATION

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.

REGISTRATION PROCESS

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 (*e.g.,* holographic devices). The applicant certificate holder may present original documentation or duly notarised and certified true copies of original documentation:

- in person or
- by mail or electronic methods.

The Registration and Authentication process of a Standard Commercial Digital Certificate Holder's identity includes:

- the Applicant Digital Certificate Holder making an in-person appearance before a Registration Authority.
- one form of government issued photographic identification is reviewed and photocopied.
- 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.

DIGITAL CERTIFICATE GENERATION

All successful Standard Commercial Digital Certificate requests will be processed by the Issuing Certification Authority. Each Standard Commercial Digital Certificate application is assigned a unique Application Identifier as the Digital Certificate is generated. The Issuing Certification Authority will apply to the Digital Certificate request a:

- Unique serial number
- Operational Certification Authority's signature

DIGITAL CERTIFICATE DELIVERY

- Download over the Internet
- CD/Floppy Disk
- Smart Card or other secure hardware token

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.

FIELDS	CONTENT	DEMARCATION
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)	aaa@bbb.xx.yy or aaa@bbb.com	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/Localitry	Variable Data	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Extensions		
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	http://www.quovadis.bm/pn	Fixed
Authority Information Access	https://www.ocsp.quovadisoffshore.com	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
CRL Distribution	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.5. Qualified Commercial Certificate

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

The primary purpose of a Qualified Digital Certificate 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.

The procedure below assumes an application by a company or organisation on behalf of its employees or counterparties for qualified Digital Certificates (similar to Employee Class A Digital Certificates).

INITIAL REGISTRATION

- Issued by QuoVadis Issuing Certification Authority.
- Registration performed by a QuoVadis Registration Authorities.

IDENTIFICATION & AUTHENTICATION

The purpose of a Qualified Commercial 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.

REGISTRATION PROCESS

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 (*e.g.,* 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.
one form of government issued photographic identification is reviewed and photocopied.
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.
All information on the applicant form and all certificate fields shown in the certificate are verified as accurate including an applicants affiliation with a commercial subject.

DIGITAL CERTIFICATE GENERATION

All successful Qualified Commercial 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:
Unique serial number
Operational Certification Authority's signature
Digital Certificate is generated and stored in a compliant S.S.C.D container - i.e. a secure/cryptographic smartcard or USB token.

DIGITAL CERTIFICATE DELIVERY

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.

FIELDS	CONTENT	DEMARCATION
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)	aaa@bbb.xx.yy or aaa@bbb.com	CH Variable
Common Name (CN)	First Name - Last Name	CH Variable
Organisational Unit (OU)	Qualified 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)	Organisation Name	CH Variable
Date Of Birth	DD/MM/YYYY	CH Variable
Place of Birth	City	CH Variable
Title	Verified Legal Title	CH Variable
Residence	ISO Country Code – Normally Resident	CH Variable
Country	ISO Country Code – Nationality	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Non Repudiation	Fixed
Private Key Usage	Validity of Private Key < Cert	CH Variable
Certificate Policies	http://www.quovadis.bm/pn	Fixed
Authority Information Access	https://www.ocsp.quovadisoffshore.com	Fixed
Subject Alternative Name	Principle Name = Email Address	CH Variable
Issuer Alternative Name	ZertES Recognition Body KPMG Klynveld Peat Marwick Goerdeler SA	Fixed
QC Statement PKIX Compliance	1.3.6.1.5.5.7.1.3	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	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.5.1 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.

INITIAL REGISTRATION

- Issued by QuoVadis Issuing Certification Authority.
- Registration performed by a QuoVadis Registration Authority.

IDENTIFICATION & AUTHENTICATION

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.

REGISTRATION PROCESS

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 (*e.g.,* 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.
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.
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.

DIGITAL CERTIFICATE GENERATION

All successful Commercial Digital Certificate requests will be processed by the QuoVadis Issuing Certification Authority. Each 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:
Unique serial number
Operational Certification Authority's signature
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.

FIELDS	CONTENT	DEMARCATION
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha1RSA	Fixed
Issuer		
Common Name (CN)	QV SCHWEIZ ICA	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink Schweiz AG	Fixed
Country (C)	CH	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 (OelDI)/Third Party Services (Art.9 OelDI)	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
Extensions		
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	http://www.quovadis.bm/pn	Fixed
Policy Qualifier User Notice	*gestuetzt auf Art. 12 Abs. 1 EIDI-V (SR 641.201.1);* *en vertu de l'art. 12 al. 1 OelDI (RS 641.201.1);* *visto l'art. 12 cpv. 1 OelDI (RS 641.201.1);* *based on art. 12 para. 1 OelDI (SR 641.201.1).*	Fixed
Authority Information Access	https://ocsp.quovadisoffshore.com	Fixed
Issuer Alternative Name	O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA	Fixed
CRL Distribution	http://www.quovadisoffshore.com/trust/qvtsagca.crl	Fixed
Thumbprint Algorithm	sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	www.quovadis.bm/policies	Fixed

10.1.6. Device Digital Certificates

FIELDS	CONTENT
Version	Version 3
Serial Number	Unique Number System Generated
Signature Algorithm	Sha1RSA
Issuer	
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
Subject	
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com
Common Name (CN)	First Name - 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
Extensions	
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	http://www.quovadis.bm/pn
Authority Information Access	https://www.ocsp.quovadisoffshore.com
Subject Alternative Name	Principle Name = Email Address
CRL Distribution	http://www.ocsp.quovadisoffshore.com/crl/CAname.crl
Thumbprint Algorithm	Sha1
Thumbprint	System Generated
Policy Notice	www.quovadis.bm/policies

10.1.7 Closed Community Certificates

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

Certificates issued under closed community certification authorities are for reliance by members of that community only, and as such a closed community certification authority can, by publication of a standalone 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 Certificate Policy & Certification Practice Statement.

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

11 APPENDIX B
11.1 Definitions and Interpretation

In this QuoVadis Certificate Policy & Certification Practice Statement the following Key terms and Abbreviations shall have the following meaning in the operation of the QuoVadis Public Key Infrastructure 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 involved in the day to day operations of a Certification Authority.

"**Certificate Policy & Certification Practice Statement"** is a publicly available document that details the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure.

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

"**Certificate Policy**" means a certificate policy adopted by an Issuing Certificate Authority operating within the QuoVadis Public Key Infrastructure 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 Public Key Infrastructure that: (i) identifies the Issuing Certification Authority; (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 Certification Authority; and

(vi) has prescribed Key Usages and Reliance Factor that governs its issuance and use whether expressly included or incorporated by reference to this Certificate Policy & Certification Practice Statement.

"**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**" means a Certification Authority duly authorised to operate by QuoVadis to issue Digital Certificates to Certificate Holders within the QuoVadis Public Key Infrastructure.

"**Issuing Certification Authority Agreement**" an agreement entered into between QuoVadis and an Issuing Certification Authority to provide Issuing Certification Authority services within the QuoVadis Public Key Infrastructure.

"**Issuing Certification Authority Certificate**" A Digital Certificate issued by the QuoVadis Root Certification Authority to an Issuing Certification Authority enabling that Issuing Certification Authority 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 Public Key Infrastructure and include (i) Issuing Certification Authorities 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.

"**Policy Management Authority**" means the QuoVadis body responsible for overseeing and approving Certificate Policy & Certification Practice Statement 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 Public Key Infrastructure.

"**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**" 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 Certification Authority.

"**QuoVadis Public Key Infrastructure**" means the infrastructure implemented and utilized 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 Public Key Infrastructure responsible for identification and authentication of Certificate Holders.

"**Registration Authority Agreement**" an agreement entered into between an Issuing Certification Authority and a Registration Authority pursuant to which that Registration Authority is to provide its services within the QuoVadis Public Key Infrastructure.

"**Registration Authority Certificate**" means a digital identifier issued by an Issuing Certification Authority (including QuoVadis in its capacity as an Issuing Certification Authority) in connection with the establishment of a Registration Authority within the QuoVadis Public Key Infrastructure.

"**Registration Authority Officer**" means an Individual designated by a Registration Authority as being authorized 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 Digital Certification Authority being a self-signed Digital 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 Public Key Infrastructure.

"**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).