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: **03 April 2007**

Version: **4.3**

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

Table of Contents

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

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 anyd(cieh lev.207 Td(and)Tj/C2020re a0.)]TJ7.0.000ormi7 TDEe -1.207 Td<0078>Tj/TT1 1 Tf( )Tj/TT2 1 Tf-0.0001 Tc Tc

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 oth549.j0.0006 P2 saclctory

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

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

1.3.9. Other Participants

Other Participants in the QuoVadis Public Key Infrastructure are required to act in accordance with this Certificate

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

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 Certif

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 Au

3.3.1. Identification And Authentication For Routine Re-Key

Identification and Authentication for rout

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 aCerh88C;rtig77 Tw -26.3 0004

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.

4.9.16. 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 Subscript/1 refo(e Tw -0 -1.2((u)-2(st bt/1 r3r)-7(or)]T Arc7plc2)]TtTJ/5h Of)4218YOn Susp01-1.2

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 peopg4(p)d2g audit lw T*ye1 1 tatio2e967 ived 67 ived 6

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.

5.3.7. 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

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.

- 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

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. ItKeys [(Digital Ce-0.0006 Tc 0. 0 9 72 2878c Tc k4.hpr(esc)]TJ-0.01 Tc 0.0009 T5 Tw [(rlcQ4 Tc eTw 25.19iuon Authority)-8( )

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.

Tw 1(30.000o118.1)vat108000 Keysi-1(rtK6w -40.06 -1y)5rtK6ve

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

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

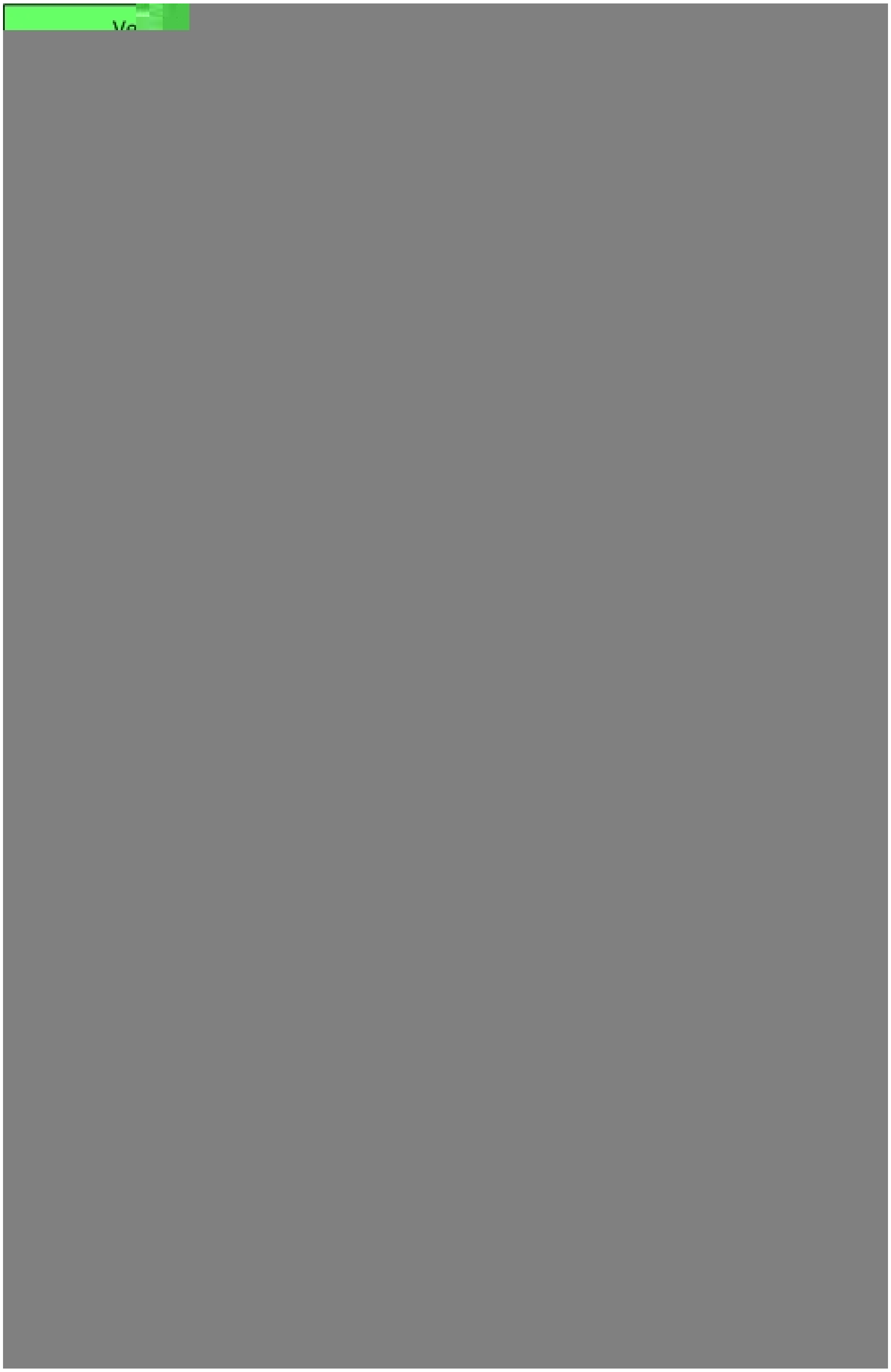
7.1. Certificate Profile

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:

7.5. 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	scnn8 43.4nS6B10.8q.J0re0o[(scn4-1caF1o[(S6g-5( )].16 5n70.0001 l144 597.54 llclP0.010 crefmmmmmmm10 cn

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:

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

Field	QuoVadis Issuing CA 3

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

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 B7.4 29	6.7001 m(Field)Tj Ce Tf Object5ield 7.4 294.84 66ieldc des5 s

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

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

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

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

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;

- 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

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

Quo

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

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.

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 QuoV

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		

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 photograph

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

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.

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.
[illegible]7.4 489.s2a3(9e re-0i tr06.707 0 le4762pq7Q8emS()Sogal7 rec 0.oawf0iun

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

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.

Organisational Unit (OU)	Not Stipulated	CH Variable
Organisational Unit (OU)	Accounting Services (OeIDI)/Third Party Services (Art.9 OeIDI)	Fixed
Organisation (O)	Organisation Name	CH Variable
Locality (L)	Not Stipulated	CH Variable
State/Province (SP)	Not Stipulated	CH Variable
Country (C)	Not Stipulated	CH Variable
Subject Public Key Information	RSA (1024/2048 bit) / System Generated	Fixed
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 OeIDI (RS 641.201.1);
	visto l'art. 12 cpv. 1 OeIDI (RS 641.201.1);
	based on art. 12 para. 1 OeIDI (SR 641.201.1).
		Fixed

Authority Information Access		

10.1.6. Special Purpose Certificates

INITIAL REGISTRATION

-

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

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

(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.

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).