QUOVADIS ROOT CERTIFICATION AUTHORITY CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT

OID: 1.3.6.1.4.1.8024.0.1
Effective Date: 14 September 2006
Version: 4.1

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

Table of Contents

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 Certificate. 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 its Root Certificate. Issuing Certificates are only issued to Approved Issuing Certification Authorities. An Approved Issuing Certification Authority utilises its Issuing Certificate to create, sign and issue Certificate Holder Digital Certificates. Approved Registration Authorities act as the interface between Issuing Certification Authorities and an Applicant Digital Certificate Holder. Approved Registration Authorities perform due diligence on potential Digital Certificate Holders and only successful applicant Digital Certificate Holders are approved and receive a Certificate Holder Digital Certificate.

Authorised Issuing Certification Authorities 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:

- Registration Authorities
- Digital Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance
-

1.3.8.1. Obligations and Responsibilities

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.

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

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

Website: www.quovadis.bm
Electronic mail:

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)
-

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.

3.3.2. 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 Certif 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

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

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 Infrastructu

- 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

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.

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

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.

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.

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 fo5o8 0.40]TJ6.24 640.tion

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

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 ific5e7on 5.1

- Is the version intended for use

The QuoVadis Chief Security Officer periodically verifies the integrity of the Certificate Authority software and

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 Identifier (OID) assigned to this Certificate Policy & Certification Practice Statement is 1.3.6.1.4.1.8024.0.1.

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 the Object Identifier 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

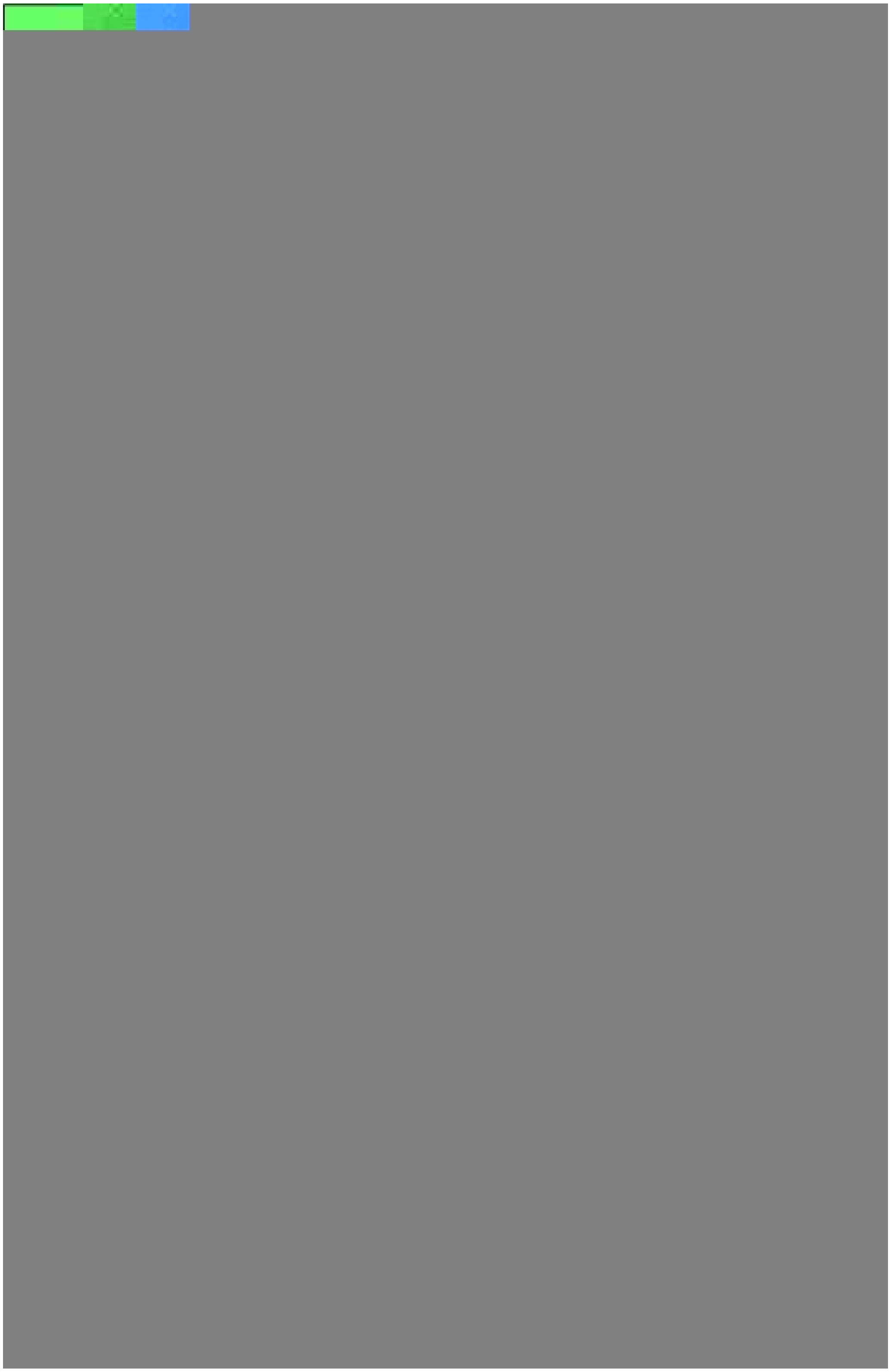
LDAP V3 in accordance with RFC-3377

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



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

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

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 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

Validity	ThisUpdate: Month/Day/Year NextUpdate: Month/Day/Year
Extensions	CRL Extensions: 3 2.5.29.20: Flags = 0, Length = 3 CRL Number CRL Number=# 2.5.29.35: Flags = 0, Length = a6 Authority Key Identifier KeyID=8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Certificate Issuer: Directory Address: CN=QuoVadis Root Certification Authority OU=Root Certification Authority O=QuoVadis Limited

Field	QuoVadis Root CA CRL
	C=BM Certificate SerialNumber=3a b6 50 8b 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

8.1.2. 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:

¢ [illegible]

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

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 financ

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:

-

- 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

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 drafil Poli41gita.TDp04

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:

-

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		

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		

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		

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	

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 informationard.

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.

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

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

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 Cloic

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

“**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).