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:	**27 May 2008**
Version:	**4.5**

Table of Contents

1. INTRODUCTION 1
1.1. Overview 1
1.2. Document Name, Identification and Applicability 2
1.3. Public Key Infrastructure Participants 2
1.4. Certificate Usage 8
1.5. Policy Administration 9
1.6. Definitions and Acronyms 9
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 9
2.1. Repositories 9
2.2. Publication of Certificate Information 10
2.3. Time or Frequency of Publication 10
2.4. Access Controls on Repositories 10
3. IDENTIFICATION AND AUTHENTICATION 10
3.1. Naming 10
3.2. Initial Identity Validation 11
3.3. Identification And Authentication For Renewal Requests 13
3.4. Identification and Authentication For Revocation Requests 13
4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS 14
4.1. Certificate Application 14
4.2. Certificate Application Processing 14
4.3. Certificate Issuance 15
4.4. Certificate Acceptance 15
4.5. Key Pair And Certificate Usage 16
4.6. Certificate Renewal 16
4.7. Certificate Re-Key 17
4.8. Certificate Modification 17
4.9. Certificate Revocation And Suspension 18
4.10. Certificate Status Services 20
4.11. End Of Subscription 20
4.12. Key Archival And Recovery 20
5.

1. INTRODUCTION

1.1. Overview

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

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

🇨🇭	With the exception of Certification Authorities issuing Qualified Certificates in accordance with Swiss Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing Certification Authority and Registration Authority services within the QuoVadis PKI.
🇪🇺 🇳🇱	With the exception of Certification Authorities issuing Qualified Certificates in accordance with European/Dutch Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing Certification Authority and Registration Authority services within the QuoVadis PKI.

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

- Authorised Certification Service Provider (Bermuda) entitled to issue accredited certificates under the requirements of the Electronic Transactions Act 1999. This authorisation synthesises elements of the ISO 17799 Code of Practice for Information Security Management and the European Electronic Signature Standardisation Initiative, as well as the WebTrust for Certification Authorities programme.

- WebTrust for Certification Authorities, conducted by Ernst & Young. This audit is consistent with standards promulgated by the American National Standards Institute, the Internet Engineering Task Force, and other bodies. It references the ANSI X9.79 Public Key Infrastructure Practices and Policy Framework (X9.79) standard for the financial services community and the American Bar Association's Public Key Infrastructure Assessment Guidelines.

- Qualified Certification Service Provider (Switzerland) entitled to issue and administer qualified electronic certificates, conducted by KPMG. This includes certification to SR 943.03 (ZertES), ETSI TS 101.456 (Policy requirements for Digital Certification Authorities issuing Qualified Digital Certificates) and other standards.

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

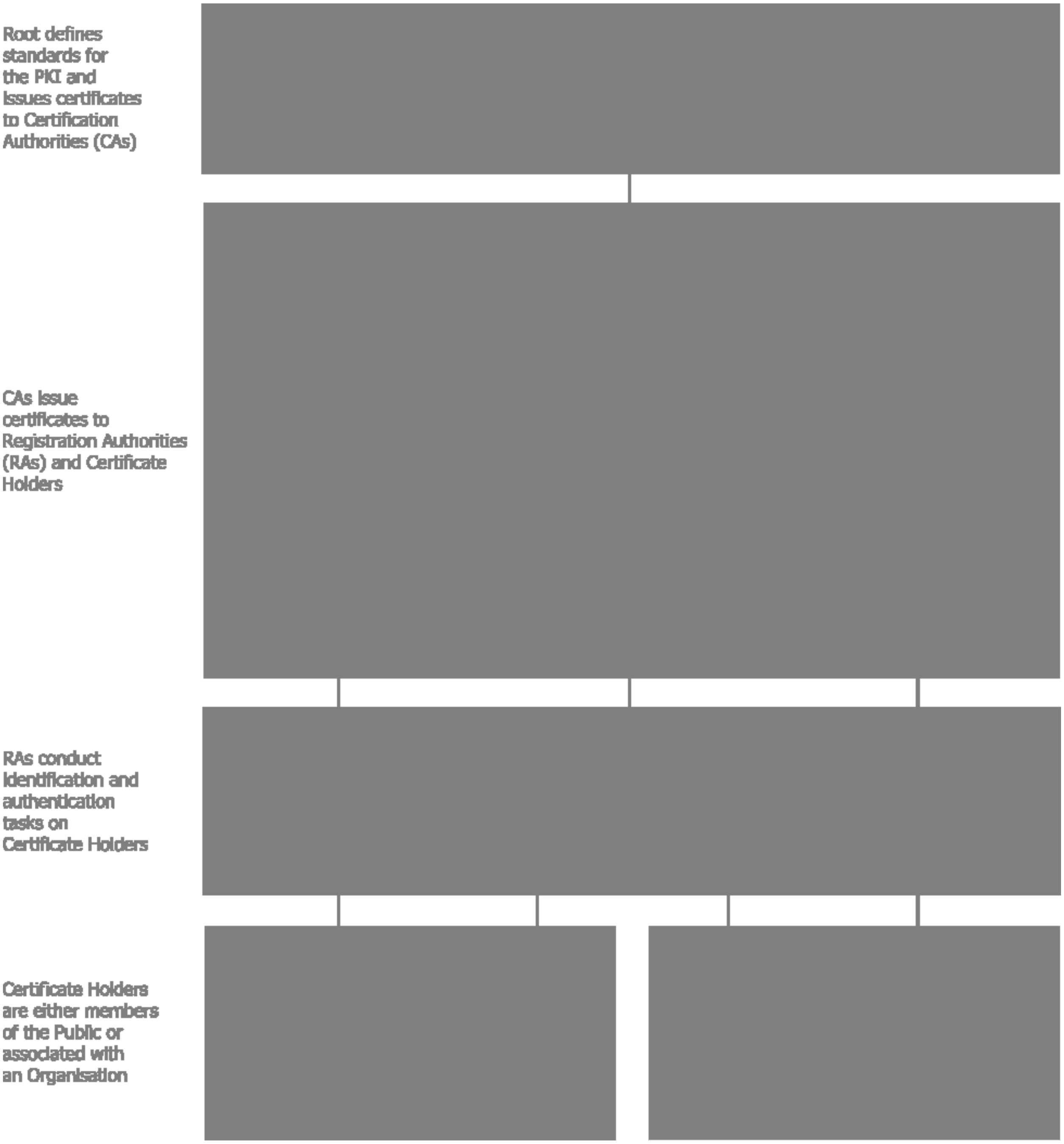
The QuoVadis PKI is designed and is operated to comply with the broad strategic direction of existing international standards for the establishment and operation of a Public Key Infrastructure Certification Authority. Any person seeking to rely on Digital Certificates or participate within the QuoVadis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

This CP/CPS undergoes a regular review process and is subject to amendment as prescribed by the QuoVadis Policy Management Authority.

The structure of this CP/CPS is based on the RFC 3647 Certificate Policy and Certification Practices Framework, but does not seek to adhere to or follow it exactly.

Any and all references to a Certificate Policy within every aspect the QuoVadis PKI refers to policies contained in the current and in-force CP/CPS.

The diagram below illustrates the components of the QuoVadis PKI:


Root defines standards for the PKI and issues certificates to Certification Authorities (CAs)
CAs issue certificates to Registration Authorities (RAs) and Certificate Holders
RAs conduct identification and authentication tasks on Certificate Holders
Certificate Holders are either members of the Public or associated with an Organisation

QuoVadis provides identification and authentication services for Digital Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this CP/CPS and in Appendix A define the credentials necessary to establish the identity of an individual or entity.

- They follow a privacy policy in accordance with this CP/CPS and applicable Issuing Certification Authority Agreement.

1.3.2. Registration Authorities and Their Obligations

Issuing CAs may, subject to the approval of QuoVadis, designate specific QuoVadis Registration Authorities to perform the Identification and Authentication and Digital Certificate request and

1.3.3.2. Accepted Limitation Of Liability

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

1.3.4. Relying Parties

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to become an "Authorised Relying Party" as defined in this CP/CPS, a Relying Party must exercise Reasonable Reliance as set out in this section 1.3.4.

All obligations within this section 1.3.4 relate to Reasonable Reliance on the validity of a Digital Signature, not the accuracy of the underlying electronic record.

This CP/CPS does not require a Certificate Holder to ensure that potential relying parties are compliant with the requirements to be an Authorised Relying Party.

1.3.4.1. Obligations and Responsibilities

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

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

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

1.3.4.2. [illegible]

1.3.4.3. Accepted Limitation Of Liability

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

1.3.4.4. Assumptions About A Certificate Holder

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

1.3.4.5. Certificate Compromise

A party cannot rely on a Digital Certificate issued by QuoVadis if the party has actual or constructive notice of the compromise of the Digital Certificate or its associated Private Key. Such notice includes but is not limited to the contents of the Digital Certificate and information incorporated in the Digital Certificate by reference, which includes this CP/CPS and the current set of revoked Digital Certificates published by QuoVadis--certificates have pointers to URLs where QuoVadis publishes status information, including Certificate Revocation Lists (CRLs), and Relying Parties are required to check the most recent CRL for certificate revocation.

1.3.5. Other Participants

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant QuoVadis documentation. All application software and operating system vendors with whom QuoVadis has entered into a contract for inclusion of the QuoVadis Root Certificate as a trusted root certificate in their software are intended third party participants in the QuoVadis PKI.

1.4. Certificate Usage

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

1.4.1. Appropriate Certificate Usage

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

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

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

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

1.4.2. Prohibited Certificate Usage

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

🟥	According to Swiss Digital Signature law (ZertES), TAV SR 943.032.1 and ETSI TS 101 456 the only appropriate use for Qualified Digital Certificates is signing.
🇪🇺 🇳🇱	According to European/Dutch Digital Signature law and ETSI TS 101 456 the only appropriate use for Qualified Digital Certificates is signing.

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

1.5. Policy Administration

1.5.1. Organisation Administering the CP/CPS

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

1.5.2. Contact Person

2.2. Publication of Certificate Information

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

2.3. Time or Frequency of Publication

Digital Certificate information is published promptly following generation and issue and immediately following the completion of the revocation process.

2.4. Access Controls on Repositories

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

3. IDENTIFICATION AND AUTHENTICATION

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

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

3.1. Naming

3.1.1. Types Of Names

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

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

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

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

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

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

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

- Email address
- Organisational Unit
- Locality

🇨🇭	For Qualified Certificates, in accordance with the Swiss Digital Signature law, all certificate fields and registration information are verified by appropriate documentation.
🇪🇺 🇳🇱	For Qualified Certificates, in accordance with the European/Dutch Digital Signature law, all certificate fields and registration information are verified by appropriate documentation.

3.2.5. Validation Of Authority

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

3.2.6. Criteria For Interoperation

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

3.3. Identification And Authentication For Renewal Requests

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

3.3.1. Identification And Authentication For Routine Re-Key

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

3.3.2. Identification and Authentication For Re-Key After Revocation

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

3.4. Identification and Authentication For Revocation Requests

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

3.4.1. Issuing Certification Authority

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

3.4.2. Registration Authority

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

3.4.3. Certificate Holder

A Digital Certificate Holder may request that his or her Digital Certificate be revoked by:

- Applying in person to the Registration Authority, Issuing CA or QuoVadis supplying either original proof of identification in the form of a valid Driving License or Passport;

🇨🇭

4.2.3. Time To Process Certificate Applications

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

4.3. Certificate Issuance

4.3.1. Certification Authority Actions During Certificate Issuance

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

4.3.1.1. QuoVadis Root Certification Authority

The Root Certification Authority Certificate has been self-generated and self-signed.

4.3.1.2. QuoVadis Issuing Certification Authority Certificates

Upon accepting the terms and conditions of the QuoVadis Issuing Certification Authority Agreement by the Issuing CA, successful completion of the Issuing Certification Authority application process as prescribed by QuoVadis, and final approval of the application by the QuoVadis Root Certification Authority, the QuoVadis Root Certification Authority issues the Issuing Certification Authority Digital Certificate to the relevant Issuing CA.

4.3.1.3. QuoVadis Registration Authority Appointment

Upon accepting the terms and conditions of the QuoVadis Registration Authority Agreement, successful completion of the Registration Authority application process and final approval of the application by the nominating Issuing CA, the Registration Authority becomes duly appointed, and appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

4.3.1.4. Registration Authority Officer's Certificate

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

4.3.1.5. Certificate Holder Certificates

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

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

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

4.4. Certificate Acceptance

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

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

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

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

4.4.1. Notice Of Acceptance

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

4.4.2. Conduct Constituting Certificate Acceptance

The downloading, installing or otherwise taking delivery of a Digital Certificate constitutes acceptance of a Digital Certificate within the QuoVadis PKI.

4.4.3. Publication Of The Certificate By The Certification Authority

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

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

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

4.5. Key Pair And Certificate Usage

4.5.1. Certificate Holder Private Key And Certificate Usage

Within the QuoVadis PKI, a Certificate Holder may only use the Private Key and corresponding Public Key in the Digital Certificate for their lawful and intended use. The Digital Certificate Holder accepts the Certificate Holder Agreement by accepting the Digital Certificate, and by accepting the Digital Certificate unconditionally agrees to use the Digital Certificate in a manner consistent with the Key-Usage field extensions included in the Digital Certificate Profile.

4.5.2. Relying Party Public Key And Certificate Usage

Any party receiving a signed electronic document may rely

- Circumstances for Digital Certificate Renewal.
- Who may request certification of a new public key.
- Processing Digital Certificate Renewal Requests.
- Notification of new Digital Certificate issuance to subscriber.
- Conduct constituting acceptance of a Renewed Digital Certificate.
- Publication of the Renewed Die.

4.9. Certificate Revocation And Suspension

4.9.1. Circumstances For Revocation

Digital certificates shall be revoked when any of the information on a Digital Certificate changes or becomes obsolete or when the private key associated with the Digital Certificate is compromised or suspected to be compromised. A Digital Certificate will be revoked in the following instances upon notification of:

- QuoVadis Certification Authority key compromise
- Digital Certificate Holder profile creation error
- Key Compromise including unauthorised access or suspected unauthorised access to private keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new certificate.
-

4.9.2.5. Application Software Vendors

An Application Software Vendor who has embedded a QuoVadis Root Certification Authority Certificate in its application as a trusted root may request the revocation of Digital Certificate chained to that Root Certificate.

4.9.3. Procedure For Revocation Request

QuoVadis will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the Issuing CA and the Registration Authority that approved or acted in connection with the issue thereof. The Digital Certificate Holder may be required to submit the revocation request via the QuoVadis Support Line or directly over an Internet connection. The Digital Certificate Holder, Registration Authority or Issuing CA may be required to provide a shared secret or pass phrase that will be used to activate the revocation process. Digital Certificate revocation requests may also be issued by contacting the administrators of the Issuing CA or Registration Authority directly. A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Holder requesting revocation (or the Organisation, where applicable). Alternatively, the Holder (or Organisation, where applicable) may request revocation by contacting the Issuing CA and providing adequate proof of identification in accordance with this QuoVadis CP/CPS or an equivalent method.

QuoVadis maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. Issuing CAs will revoke Digital Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time Within Which The Certification Authority Must Process The Revocation Request

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

4.9.6. Revocation Checking Requirement For Relying Parties

Digital Certificate revocation information is provided via the Certificate Revocation List in the QuoVadis X.500 Directory services.

4.9.7. Certificate Revocation List Issuance Frequency

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

4.9.8. Maximum Latency For Certificate Revocation List

The maximum latency for the Certificate Revocation list is 10 minutes.

4.9.9. On-Line Revocation/Status Checking Availability

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

4.9.10. On-Line Revocation Checking Requirement

The validity of a QuoVadis Digital Certificate must be checked online using the QuoVadis Repository, the appropriate Certificate Revocation list or using the appropriate Online Certificate Status Protocol responder by a Relying Party seeking to become an Authorised Relying Party.

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

4.9.11. Other Forms Of Revocation Advertisements Available

There are no other forms of Revocation Advertisements available.

4.9.12. Special Requirements Re-Key Compromise

QuoVadis does not support re-key.

4.9.13. Circumstances For Suspension

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

4.9.14. Who Can Request Suspension

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

4.9.15. Procedure For Suspension Request

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

4.9.16. Limits On Suspension Period

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

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List (http://crl.quovadisglobal.com/<caname>.crl) or is made available via Online Certificate Status Protocol checking (http://ocsp.quovadisglobal.com) where available.

4.10.2. Service Availability

Digital Certificate status services are available 24 hours a day, 7 days a week, 365 days of the year.

4.10.3. Optional Features

Online Certificate Status Protocol is available for all certificate types issued by QuoVadis Issuing CAs.

4.11. End Of Subscription

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

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

4.12. Key Archival And Recovery

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

4.12.1. Key Archival And Recovery Policy And Practices

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

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

Not Applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

QuoVadis manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with CA operations wherever those operations physically occur.

5.1.1. Site Location and construction

QuoVadis performs its CA operations from a secure datacentre located in an office complex in Bermuda. The

5.1.3. Power And Air-Conditioning

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

5.1.4. Water Exposures

The QuoVadis secure operating area provides protection against water. It is located on an upper floor with raised flooring, floors and walls are sealed, and the enclosure meets the requirements of DIN 18095.

5.1.5. Fire Prevention And Protection

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

5.1.6. Media Storage

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

5.1.7. Waste Disposal

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

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

5.1.8. Off-Site Backup

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

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

5.2. Procedural Controls

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

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

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

5.2.1. Trusted Roles

In order to ensure that one person acting alone cannot circumvent security safeguards, responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. Oversight may be in the form of a person who is not directly involved in issuing Digital Certificates (e.g. a security officer) examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy. The roles defined by this CP/CPS are:

Certification Authority Officers who are responsible for CA hardware and software and the generation and signing of Issuing CA Keys.
Registration Authority Officers who are appointed by Registration Authorities, issued Registration Authority Certificates, and given responsibility for the operation of Registration Authority functions and the interface with the Issuing CA.

QuoVadis Chief Security Officer who is responsible for verifying the integrity of the Certification Authorities and Registration Authorities and their operations and configurations.

5.2.2. Number of Persons Required Per Task

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

CA key-pair generation and initialisation of a Root CA or Issuing CA shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

Issuing CAs will utilise commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. Issuing CAs must ensure that no single individual may gain access to any Private Key (other than the individual's own Private Key). At a minimum, procedural or operational mechanisms must be in place for Issuing CA key recovery in disaster recovery situations. To best ensure the integrity of the Issuing CA equipment and operation, Issuing CAs will use commercially reasonable efforts to identify a separate individual for each trusted role.

5.2.3. Identification and Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure, designated "Position of Trust".

Each individual performing any of the trusted roles shall use a QuoVadis issued Digital Certificate (i.e. a Utility Certificate) stored on a cryptographic smart card evaluated to at least Common Criteria EAL 4 to identify themselves to the Digital Certificate server and Repository.

5.2.4. Roles Requiring Separation of Duties

Operations involving Root Certificate and Issuing CA roles are segregated between M of N employees where M is equal to or greater than 2. (An M-of-N person control means there is a minimum "M" persons present out of a total "N" persons authorised to perform the task.) Creation and maintenance of system audit logs are segregated from those persons who operate such systems.

5.3. Personnel Controls

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

For purposes of mitigating the risk that one individual acting alone could compromise the integrity of the QuoVadis PKI or any Digital Certificate issued therein, QuoVadis performs relevant background checks of individuals and defines the tasks that the individuals will be responsible to perform. QuoVadis determines the nature and extent of any background checks, in its sole discretion. The foregoing fully stipulates QuoVadis' obligations with respect to personnel controls, and QuoVadis shall have no other duty or responsibility with respect to the foregoing. Without limitation, QuoVadis shall not be liable for employee conduct that is outside of their duties and for which QuoVadis has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.1. Qualifications, Experience, and Clearance Requirements

QuoVadis requires that personnel meet a minimum standard with regards to Qualifications, Experience, Clearance and Training.

5.3.2. Background Check Procedures

Background check procedures include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Criminal Records
- Credit/financial history and status
- Driving licenses

- Audit Opinions as discussed in this QuoVadis CP/CPS; and
- Name of the relevant QuoVadis Registration Authority.

5.5.2. Retention Period For Archive

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

5.5.3. Protection Of Archive

Archives shall be retained and protected against modification or destruction. Only Certification Authority Officers, the QuoVadis Chief Security Officer, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.5.4. Archive Backup Procedures

QuoVadis maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

5.5.5. Requirements For Time-Stamping Of Records

QuoVadis retains the right to generate the Digital Certificate Holder's public and private key pair. The Digital Certificate Holder is required to provide all the necessary identification and authentication information when the Digital Certificate is being requested. Once all of the registration information is collected by the QuoVadis Certification Authority, the Digital Certificate Holder's public and private key pair are generated within a secure environment. QuoVadis Digital Certificate Holders can generate their own private key prior to submitting a Digital Certificate request. Key Generation methods and requirements differ according to the type of Digital Certificate requested.

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

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

6.1.2. Private Key Delivery To Certificate Holder

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

6.1.3. Public Key Delivery To Certificate Issuer

Public Keys must be delivered in a secure and trustworthy manner, such as a Digital Certificate request message. Delivery may also be accomplished via non-electronic means. These means may include, but are not limited to, USB drive (or other storage medium) sent via registered mail or courier, or by delivery of a Token for local Key generation at the point of Digital Certificate issuance or request. Offline means will include Identity checking and will not inhibit establishing proof-of-possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a Certificate Holder Agreement or other agreement. In those cases where Key Pairs are generated by the Issuing CA on behalf of the Holder, the Issuing CA will implement secure mechanisms to ensure that the Token on which the Key Pair is held is securely sent to the proper Holder, and that the Token is not activated prior to receipt by the proper Holder.

6.1.4. Certification Authority Public Key To Relying Parties

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

6.1.5. Key Sizes

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

6.1.6. Public Key Parameters Generation And Quality Checking

For Certificate Holders, the quality of parameters used to create Public Keys are determined by the relevant Registration Authority application or by the Certificate Holder's client application.

For QuoVadis, its Issuing CAs and Registration Authorities, all hardware and associated software platforms meet the requirements of FIPS 186-2, which ensures the proper parameters and their quality (e.g. random-generation and primality).

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

Keys may be used for the purposes and in the manner described in the QuoVadis CP/CPS – Digital Certificate Profiles.

An Issuing CA's Private Keys may be used for Digital Certificate signing and CRL and OCSP response signing. Keys may also be used to authenticate the Issuing CA to a Repository.

6.2. Private Key Protection And Cryptographic Module Engineering Controls

🇨🇭 🇪🇺 🇳🇱	Under no circumstances will private keys for Qualified Digital Certificates be archived.

6.2.6. Private Key Transfer Into Or From A Cryptographic Module

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

6.2.7. Private Key Storage On Cryptographic Module

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

6.2.8. Method Of Activating Private Key

A Digital Certificate Holder must be authenticated to the Cryptographic Module before the activation of the Private Key. This Authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

6.2.9. Method Of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorised access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the Holder's sole control. Issuing CA private keys are not usually deactivated, but are kept in locked computer cabinets with appropriate physical and logical security controls. Other cryptographic modules used by QuoVadis are deactivated through a manual logout procedure or a passive timeout.

6.2.10. Method Of Destroying Private Key

Private Keys should be destroyed when they are no longer needed, or when the Digital Certificates to which they correspond expire or are revoked.

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

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

6.2.11. Cryptographic Module Rating

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

🇨🇭	For Qualified Certificates, in accordance with Swiss Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 standards.
🇪🇺 🇳🇱	For Qualified Certificates, in accordance with European/Dutch 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

6.5.2. Computer Security Rating

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

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

6.6. Life Cycle Technical Controls

All hardware and software procured for operating an Issuing CA within the QuoVadis PKI must be purchased in a manner that will mitigate the risk that any particular component was tampered with, such as random selection of stamp Authority such that Participants and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

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

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

All QuoVadis Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilise the ITU-T X.509 version 3 Digital Certificate standard.

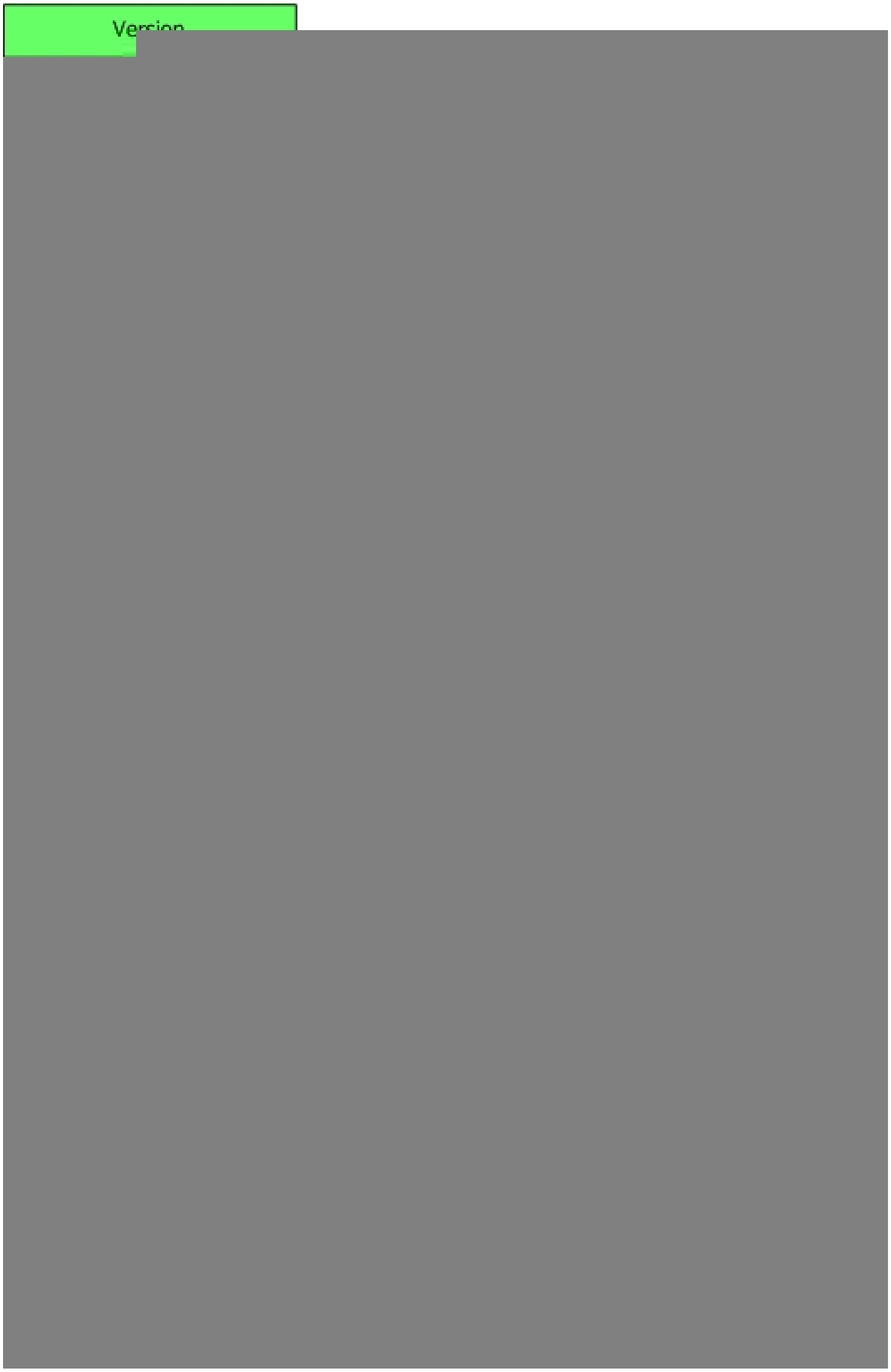
Digital Certificate profiles within the QuoVadis PKI are detailed in Appendix A.

7.3. Online Certificate Status Protocol Profile

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

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
Serial Number	3ab6508b
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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency, Circumstance And Standards Of Assessment

8.1.1. QuoVadis Certification Authority

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

Standards / Law	
Bermuda Accredited Certificate Service Provider	As defined in Bermuda's Electronic Transactions Act 1999, an Authorised Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.
WebTrust for Certification Authorities	The WebTrust Seal of assurance for Certification Authorities (CA) symbolises to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria.
SR 943.03 [ZertES]	Dated 21 December 2004 Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der (qualifizierten) elektronischen Signatur
SR 943.032 [VZertES]	Dated 6 December 2004 TAV Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur
SR 943.032.1 [TAV]	Dated 6 December 2004 (Ausgabe 1: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur („zur Anerkennung für qualifizierte elektronische Zertifikate" nach Kapitel 2)
ESI ("Directive")	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
ETSI [ESTI101456TS]	

8.3. Assessor's Relationship To Assessed Entity

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

8.4. Topics Covered By Assessment

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

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

8.5. Actions Taken As A Result Of Deficiency

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

🟥	For Qualified Certificates, in accordance with the Swiss Digital Signature law, the course of action and time frame for rectification of any deficiency as set by the accrediting authority Metas-SAS must be followed.
🇪🇺 🇳🇱	For Qualified Certificates, in accordance with the European/Dutch law, the course of action and time frame for rectification of any deficiency as set by the independent reviewing party must be followed.

to termination of that Issuing CA’s or Registration Authority’s agreement with QuoVadis and the associated revocation of any Digital Certificate issued to them; (iii) limit the class of any Digital Certificates issued by the Nominating Issuing CA; or (iv) terminate that Issuing

9.2.2. Other Assets

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

9.2.3. Insurance Or Warranty Coverage For End-Entities

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

9.4.2.1. Registration Records

All registration records are considered confidential information and treated as private.

9.4.2.2. Certificate Revocation

Except for reason codes contained in a Certificate Revocation List, the detailed reason for a Digital Certificate being revoked, (if applicable), is considered to be confidential information, with the sole exception of the revocation of an Issuing CA's Issuing Certificate due to:

- the compromise of the Issuing CA's Private Key, in which case a disclosure may be made that the Private Key has been compromised;
- the termination of a Issuing CA within the QuoVadis 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.

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

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

9.4.6.2. Release As Part Of Civil Discovery

As a general principle, no document or record belonging to QuoVadis is released to any person except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to QuoVadis to be under appeal when served on QuoVadis (QuoVadis being under no obligation to determine the same), and which has been determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the relevant CA and enforceable in that jurisdiction or enforceable under the laws otherwise governin(tion)]TJ0e9-8(ictJr.odu)-3(c)1-utio-0.0001A anin0m 26.713 0 Tdrlawd2

    - within applicable law and regulation;
- approving the establishment of all Issuing CAs and on approval, executing an Issuing CA Agreement (save in respect of the QuoVadis Issuing CA);
- maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation;
- publishing its QuoVadis CA Certificates at www.quovadisglobal.com/repository and other nominated web sites;
- issuing CA Certificates to Issuing CAs that comply with X.509 standards and are suitable for the purpose required;
- issuing CA Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
- publishing issued Issuing CA Certificates without alteration in the X.500 Directory;
- investigating any suspected compromise which may threaten the integrity of the QuoVadis PKI;
- revoking Issuing CA Certificates and posting such revoked Certificates in the X.500 Directory Certificate Revocation List; and
- conducting compliance audits of Issuing CAs.

9.6.1.2. Issuing Certification Authority Warranties

An Issuing CA hereby warrants (a) it has taken reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue, and (b) Digital Certificates shall be revoked if the Issuing CA believes or is notified that the contents of the Digital Certificate are no longer accurate, or that the key associated with a Digital Certificate has been compromised in any way.

The nature of the steps the Issuing CA takes to verify the information contained in a Digital Certificate vary according to the Digital Certificate fee charged, the nature and identity of the Digital Certificate Holder, and the applications for which the Digital Certificate will be marked as trusted. The Issuing CA makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

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

9.6.2. Registration Authority Representations and Warranties

9.6.2.1 Representations

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

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

9.6.2.2 Warranties

Authorised Registration Authorities operating within the QuoVadis PKI hereby warrant that (a) they take reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue, and (b) they will request that Digital Certificates be revoked by QuoVadis if they believe or are notified that the contents of the Digital Certificate are no longer accurate, or that the key associated with a Digital Certificate has been compromised in any way.

9.6.3. Certificate Holder Representations And Warranties

- They will promptly request revocation of the Digital Certificate in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key listed in the Digital Certificate.

9.6.4. Relying Parties Representations And Warranties

Relying Parties represent and warrant that:

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

9.6.5. Representations And Warranties Of Other Participants

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

9.7. Disclaimers Of Warranties

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

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

9.8. Liability and Limitations of Liability

9.8.1. QuoVadis Liability

QuoVadis shall be liable to Digital Certificate Holders or relying parties only for direct loss arising from any breach of this CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit specified below in section 9.8.3.1 for any one event or series of related events (in any one twelve-month period).

🇨🇭	For Qualified Certificates, in accordance with the Swiss Digital Signature law, namely, Art 16 of Zert ES: 1. QuoVadis is liable to the Certificate Holder or the Relying Party who relies on a valid Qualified Certificate, for damages that arise because QuoVadis has not followed the procedures required by ZertES. 2. QuoVadis has the obligation to prove that such procedures were followed in accordance with ZertES. 3. QuoVadis cannot disclaim liability to either the Certificate Holder or Relying Party except where the Certificate Holder or Relying Party has not complied with the terms and conditions of use of the Certificate. Sections 9.8.2; 9.8.3; 9.8.4; 9.8.5 DO NOT apply to Qualified Certificates.
🇪🇺 🇳🇱	For Qualified Certificates, in accordance with the European/Dutch Digital Signature law, QuoVadis is liable under: • The Dutch Electronic Signatures Act of 8 May 2003 (entered into force on 21 May 2003) • The Dutch electronic signature regulation "Besluit Elektronische Handtekeningen (Stb. 2003, 200)" • Article 6 of "European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures"

9.8.2. QuoVadis' Limitations Of Liability

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

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

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 activ1938n003 Tc 0.0otheor activ

[redacted]

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

🇨🇭	For Qualified Certificates, in accordance with the Swiss Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in Switzerland.
🇪🇺 🇳🇱	For Qualified Certificates, in accordance with Dutch Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in The Netherlands.

9.14. Governing Law

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

- Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.
- Dispute between an IssuingDC ite .0004jEMC /F follows; XN?@€

9.16.5. Force Majeure

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

9.17. Other Provisions

10. APPENDIX A

10.1. Digital Certificate Profiles

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

10.1.1. Standard Test Certificate

INITIAL REGISTRATION

Key Usage	Data Encipherment (Optional)	Holder Variable
Key Usage	Key Agreement (Optional)	Holder Variable

Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature (Optional)	Holder Variable
Key Usage	Non Repudiation (Optional)	Holder Variable
Key Usage	Key Encipherment (Optional)	Holder Variable
Key Usage	Data Encipherment (Optional)	Holder Variable
Key Usage	Key Agreement (Optional)	Holder Variable
Enhanced Key Usage	Client Authentication (Optional)	Holder Variable
Enhanced Key Usage	Secure Email (Optional)	Holder Variable
Enhanced Key Usage	Encrypting File System (Optional)	Holder Variable
Enhanced Key Usage	Smart Card Logon (Optional)	Holder Variable
Certificate Policies	http://quovadisglobal.com/repository	Fixed
Authority Information Access	http	

State or Province	Not Stipulated	Holder Variable
Country	ISO Country Code	Holder Variable
Date Of Birth	DD/MM/YYYY	Holder Variable
Place of Birth	City	Holder Variable
Gender	M/F	Holder Variable
Title	Verified Legal Title	Holder Variable
Country of Residence	ISO Country Code – Normally Resident	Holder Variable
Country of Citizenship	ISO Country Code – Nationality	Holder 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 Non Repudiation	

10.1.3 Qualified Certificate –The Netherlands

Please note that where a Qualified Personal Digital Certificate is issued within the meaning of EU Directive 1999/93/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 CA. • 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

Date Of Birth	DD/MM/YYYY	Holder Variable
Place of Birth	City	Holder Variable
Gender	M/F	Holder Variable
Title	Verified Legal Title	Holder Variable
Country of Residence	ISO Country Code – Normally Resident	Holder Variable
Country of Citizenship	ISO Country Code – Nationality	Holder Variable
Subject Public Key Information	RSA (1024/2048/4096 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 Non Repudiation	Holder Variable Fixed
Private Key Usage	Validity of Private Key < Cert	Holder Variable
Certificate Policies	http://quovadisglobal.com/repository	Fixed
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/<caname>.crt	Fixed
Subject Alternative Name	Principal Name = Email Address	Holder Variable
QC Statement PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed
QC Statement ETSI Compliance	0.4.0.1862.1.1	Fixed
Monetary Statement	0.4.0.1862.1.2	Holder Variable
SSCD Statement	0.4.0.1862.1.4	Fixed
CRL Distribution	http://crl.quovadisglobal.com/<caname>.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
Policy Notice	http://quovadisglobal.com/repository	Fixed

10.1.4. Standard Commercial Certificate

[redacted]

10.1.5 Commercial - EIDI-V Certificates

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

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

INITIAL REGISTRATION
• Issued by QuoVadis Issuing CA. • Registration performed by a QuoVadis Registration Authority.
PURPOSE
The purpose of a Commercial Advanced Digital Certificate is to identify the organisation and individl748d witc 0.0004 Tw ificate is org

•

Organisational Unit (OU)	Not Stipulated	Holder Variable
Organisational Unit (OU)	Not Stipulated	Holder Variable
Organisational Unit (OU)	Not Stipulated	Holder Variable
Organisational Unit (OU)		

10.1.6. Special Purpose Certificates

INITIAL REGISTRATION
• Issued by QuoVadis Issuing Certification Authority. • Registration performed by a QuoVadis Registration Authority.
DESCRIPTION
Special Purpose Digital Certificates include certificates issued primarily for one or more of the Extended Key Usages as shown below. These certificates may be issued to natural persons, devices or organisations.
REGISTRATION PROCESS

An application form for a Special Purpose Digital Certificates is submitted, defining the contents of the fields required to be completed. For

- Natural person: a copy of an official photo ID document with signature or the confirmation of a notary or other accredited third party regarding the correctness and the completeness of the data is required. Where applicable, the affiliation of a person named in a certificate to a stated organization must be confirmed by an authorized member of that organization, which may be verified by 5 Tc 0. .29tionl org
  x
  x

Authority Key Identifier	Directory Attributes Certificate Issuer
Subject Key Identifier	ID of Certificate Holder key
Key Usage	Digital Signature (Optional)
Key Usage	Non Repudiation (Optional)
Key Usage	Key Encipherment (Optional)
Key Usage	Data Encipherment (Optional)
Key Usage	Key Agreement (Optional)

10.1.7 Closed Community Certificates

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

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

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

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

11 APPENDIX B

11.1 Definitions and Acronyms

In this QuoVadis CP/CPS the following Key terms and Abbreviations shall have the following meaning in the operation of the QuoVadis PKI unless context otherwise requires:

“**Applicant**” means an Individual or Organisation that has su

“**Digital Certificate**

owned by or available to QuoVadis adopted or designated now or at any time hereafter by QuoVadis for use in connection with the QuoVadis PKI.

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

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

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

“**Qualified Certificate**” A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the qualification requirements defined by the applicable legal framework of the European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

“**QuoVadis**” means QuoVadis Limited, a Bermuda exempted company.

“**QuoVadis Issuing Certification Authority**” means QuoVadis in its capacity as an Issuing CA.

“**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).