Important Note About this Document
This is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited, (QuoVadis). It contains

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

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

This CP/CPS describes all subordinate services that operate under the QuoVadis Root CA, i.e. that are within the

PKI include:

x   Certification Authorities;
x   Registration Authorities;
x   Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance; and
x   Authorised Relying Parties.

The practices described or referred to in this CP/CPS:

x   accommodate the diversity of the community and the scope of applicability within the QuoVadis chain of trust; and
x   adhere to the purpose of the CP/CPS of describing the uniformity and efficiency of practices throughout the QuoVadis PKI.

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

x   are the minimum requirements necessary to ensure that Certificate Holders and Authorised Relying Parties have

This CP/CPS relates to the QuoVadis Root Certification Authority, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3. QuoVadis Root CA 2 and QuoVadis Root CA 2 G3 have a separate CP/CPS.

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

1.3.1.2   Issuing CAs and Their Obligations
Issuing CAs may be operated by QuoVadis or by other Organisations that have been authorised by QuoVadis to participate within the

QuoVadis acts as RA for all Certificates it issues in accordance with the Baseline Requirements.

1.3.3.   Certificate Holders
1.3.3.1.   Obligations And Responsibilities
Certificate Holders are required to act in accordance with this CP/CPS and Certificate Holder Agreement. A Certificate Holder represents, warrants and covenants with and to QuoVadis, Relying Parties, Application Software Vendors and the Registration Authority processing their application for a Digital Certificate that:

 x   Both as an applicant for a Digital Certificate and as a Certificate Holder,

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 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 to

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 (QuoVadis Certificate Class) of Digital Certificate being issued (See Appendix A).

3.1.   Naming
3.1.1.   Types Of Names
All 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 Certificate Holder. Each User must have a unique and readily identifiable X.501 Distinguished Name (DN). The Distinguished Name may include the following fields:

x   Common Name (CN)
x   Organisational Unit (OU)
x   Organisation (O)
x   Locality bem[())] 6m 76.1dt be rfo

the generality of the foregoing, the Identity of any Organisation that seeks to act as a Registration Authority for its

x   Sending a digitally signed email message to the Issuing Registration Authority, Issuing CA

4.2.4 Certificate Authority Authorisation (CAA)

x   Circumstances for Certificate Renewal.
x   Who may request certification of a new Public Key.
x   Processing Certificate Renewal Requests.
x   Notification of new Digital Certificate issuance to Certificate Holder.
x   Conduct constituting acceptance of a Renewed Digital Certificate.
x   Publication of the Renewed Digital Certificate by the Certification Authority.
x   Notification of Digital Certificate issuance by the Certification Authority to other entities.

4.7.   Certificate Re-Key
Certificate Re-Key is when Re

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:

   x   QuoVadis Certification Authority

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.

5.1.1.   Site Location and construction
QuoVadis performs its CA operations from a secure datacentre located in Hamilton, Bermuda. The datacentre is a purpose-built steel and composite compartment, with raised floor construction and an array of resilient security and environmental systems. QuoVadis operates under a security policy designed to deter, prevent and detect unauthorized access to the datacentre.

5.1.2.   Physical Access
QuoVadis permits entry to its secure datacentre only to security-cleared and authorised personnel, whose movements within the facility are logged and audited. A police background check forms part of the security clearance authorisation process. Physical access is controlled by dual-factor authentication using a combination of physical access cards and biometric readers.

5.1.3.   Power and Air-Conditioning
The QuoVadis secure operating area is connected to dual power feeds via a fault tolerant design. All critical components are connected to dual uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure. In the event of a power failure there is an automatic failover to a standby generator.

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.

5.1.5.   Fire Prevention and Protection
The QuoVadis secure datacentre provides protection against fire and contains with an automatic FM200 extinguishing system.

5.1.6.   Media Storage
All magnetic media containing QuoVadis PKI information, including backup media, are stored

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. Overs(c)-509eu6041

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:
- x Previous employment
- x Professional references
- x Educational qualifications
- x Criminal Records
- x Credit/financial history and status
- x Driving licenses
- x Other relevant government records (e.g. national identifiers, etc.)

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

5.3.3.   Training Requirements

QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities to the highest industry standard.

5.3.4.   Retraining Frequency And Requirements

QuoVadis provides and maintains a program of retraining in order to maintain appropriate and required levels of competency to perform job responsibilities to the highest industry standard.

5.3.5.   Job Rotation Frequency And Sequence

QuoVadis provides and maintains a program of job rotation in order to maintain appropriate and required levels of competency across key roles.

5.3.6.   Sanctions for Unauthorised Actions

Appropriate disciplinary actions are taken for unauthorised actions.

5.3.7.   Independent Contractor Requirements

QuoVadis does not support the use of independent contractors to fulfil roles of responsibility.

5.3.8.   Documentation Supplied To Personnel

QuoVadis provides personnel with all required training materials needed to perform their job function and their duties under the job rotation program. This includes specific documentation of the validation, issuance, and revocation processes for Certificates.

5.4.   Audit Logging Procedures

5.4.1.   Types Of Events Recorded

All events involved in the generation of the Certification Authority Key Pairs are recorded. This includes all configuration data used in the process.

Individuals who have access to particular Key Pairs and passwords will be audited. Key pair access will take the form of PIN-protected cryptographic smart cards. Access to the Oracle database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of two people must be present to perform certain tasks on the QuoVadis Certification Authority.

The types of data recorded by QuoVadis include but are not limited to;
- x All data involved in each individual Digital Certificate registration process
- x All data and procedures involved in the certification and distribution of Digital Certificates
- x All data relevant to the publication of Digital Certificates and Certificate Revocation Lists

Digital Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or Certificate Holder Agreement.

6.   TECHNICAL SECURITY CONTROLS
The QuoVadis Certification Authority Private Keys are protected within a hardware security module meeting at least Federal Information Processing Standard-140-2 level 3 and/or EAL 4. Access to the modules within the QuoVadis environment, including the Root and Operational Digital Certification Authorities Private Keys, are restricted by the use of token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the QuoVadis management team. Such 2-of-N allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

6.1.   Key Pair Generation And Installation
6.1.1.   Key Pair Generation
All Key Pairs will be generated in a manner that QuoVadis, in its sole discretion, deems to be secure.

QuoVadis retains the right to generate the Certificate Holder Private Key Pair. The 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 Certificate Holders Key Pair are generated within a secure environment. QuoVadis 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.

Certificate Holder Key Generation may be performed in hardware or software depending on the Digital 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 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 Keyat 5(t w3(c)-5(a)139(S)-2(ta)6(nd)-8(a)5(r49

by N-of-M control discussed above in Section 6.2.2. They are backed up under further encryption and maintained on-site and in secure off-site storage.

Certificate Holders may choose to backup their Private Keys by backing up their hard drive or the encrypted file containing their Keys.

6.2.5.   Private Key Archive
Private Keys used for encryption shall not be archived, unless the Certificate Holder or Registration Authority specifically contracts for such services.   Private Key archive is prohibited for QV Advanced+ and QV Qualified Certificates, or for any Private Key whose Key Usage is dedicated to Signing or Authentication.

Where a single Key Pair is generated for Signing and Encryption, the Private Key will only be archived on the specific request of the Certificate Holder and the corporate entity with which that Certificate Holder is affiliated.

	Under no circumstances will Private Keys for Qualified Digital Certificates be archived.

6.2.6.   Private Key Transfer Into Or From A Cryptographic Module
If a Cryptographic Module is used, the Private Key must be generated in it and remain there in encrypted form, and be decrypted only at the time at which it is being used.

another, the Private Key ee be encrypted during transport.

only.

6.2.9.   Method Of Deactivating Private Key
Cryptographic Modules that have been activated ee not be left unattended or otherwise open to unautho rised access. After use, they ee be deactivated, using, for example, a eanual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the   Issuing CA Private Keys are not usually deactivated, but are kept in locked computer cabinets with appropriate physical and logical security controls.   Other cryptographic eodules 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

by deleting

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

6.3.   Other Aspects Of Key Pair Management
6.3.1.   Public Key Archival
Public Keys will be recorded in Digital Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained.

6.3.2.   Certificate Operational Periods And Key Pair Usage Periods
Usage periods for Public Keys and Private Keys shall match the usage periods for the Digital Certificate that binds the Public Key to an Individual, Organisation, or Device. Please see the variable Issuing Certificate Authority Valid From fields in the Certificate Profiles outlined in Appendix A.

The maximum validity periods for Digital Certificates issued within the QuoVadis PKI are:

x   Root CA Certificate   30 years
x   All Issuing CA Certificates   10 years
x   Qualified Certificates   1 to 3 years
x   All other Digital Certificates   Variable

6.5.   Computer Security Controls

QuoVadis has a formal Information Security Policy that documents the QuoVadis policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

Computer security technical requirements are achieved utilising a combination of hardened security modules and software, operating system security features, internal PKI and Certificate Authority Software and physical safeguards, including security Policies and Procedures that include but are not limited to:

x   Access controls to Certificate Authority services and PKI roles, see Section 5.1
x   Enforced separation of duties for Certificate Authority Services and PKI roles, see Section 5.2
x   Identification and Authentication of personnel that fulfil roles of responsibility in the QuoVadis PKI, see Section 5.3
x   Use of cryptography for session communication and database security, mutually authenticated and encrypted SSL/TLS is used for all communications
x   Archival of Certificate Authority history and audit data, see Sections 5.4 and 5.6
x   Use of x.509 Digital Certificates for all administrators.

6.5.2.   Computer Security Rating

A version of the core Certificate Authority software used by QuoVadis has obtained the globally recognised Common Criteria EAL 4+ certification.

6.6.   Life Cycle Technical Controls

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

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

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

6.6.1.   System Development Controls

Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2.   Security Management Controls

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

6.6.3.   Life Cycle Security Controls

QuoVadis employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority systems. The Certificate Authority software, when first loaded will provide a method for QuoVadis to verify that the software on the system:

x   Originated from the software developer
x   Has not been modified prior to installation
x   Is the version intended for use

The QuoVadis Chief Security Officer periodically verifies the integrity of the Certificate Authority software and monitors the configuration of the Certificate Authority systems.

| Title (T) | Subject Title (for example Dr.) | Holder Variable |
| Generation Qualifier | Subject Generation Qualifier (for example Jr.) | |

FIELDS	CONTENT	DEMARCATION
	URL = http://ocsp.quovadisglobal.com URL=http://trust.quovadisglobal.com/<caname>.crt (where <caname> is the short name of the relevant CA)	
Basic Constraints	Indicates whether the subject of the Digital Certificate is a CA and the maximum depth of valid certification paths that include this Certificate.	Fixed
Thumbprint Algorithm	The algorithm used to hash the Certificate	Fixed
Thumbprint	The system generated hash of the Certificate	Fixed

7.1.3.   Algorithm Object Identifiers
No Stipulation.

7.1.4.   Name Forms
See 3.1.1

7.1.5.   Name Constraints
See 3.1.1

7.1.6.   CP/CPS Object Identifier
The Object Identifiers (OIDs) assigned to this CP/CPS are 1.3.6.1.4.1.8024.0.1 and 1.3.6.1.4.1.8024.0.3.

7.1.7.   Usage Of Policy Constraints Extension
No Stipulation.

7.1.8.   Policy Qualifiers Syntax And Semantics
Digital Certificates issued within the QuoVadis PKI contain one of the Object Identifiers for this CP/CPS and an Object Identifier representing the QuoVadis Certificate Class.

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

7.2.   Certificate Revocation List Profile
Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 5280.
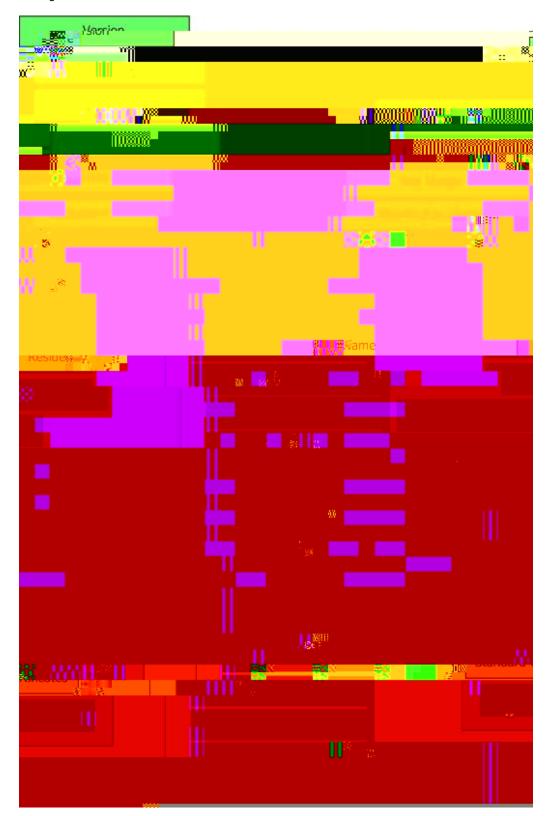
7.2.1.   Version Number
Issuing CAs within the QuoVadis PKI issue X.509 version 2 Certificate Revocation Lists.

7.2.2.   Certificate Revocation List And Certificate Revocation List Entry Extensions
All User PKI software must

7.5.   Digital Certificate Fields and Root CA Certificate Hashes
7.5.1.   Digital Certificate Fields

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

QuoVadis CAs following this CP/CPS are subject to audits in respect of its various accreditations and certifications as follows:

Standards / Law	
Bermuda Accredited Certificate Service Provider	Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.

WebTrust for Certification Authorities

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 AG.

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 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.
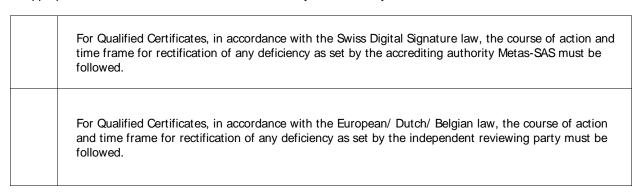
8.4.   Topics Covered By Assessment

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

x   Security Policy and Planning;
x   Physical Security;
x   Technology Evaluation;
x   Services Administration;
x   Personnel Vetting;
x   Contracts; and
x   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/ Belgian law, the course of action and time frame for rectification of any deficiency as set by the independent reviewing party must be followed.

Remedial action determined by QuoVadis shall be limited to the operations and procedures required to be taken in order to ensure that the Registration Authority operates in compliance with the QuoVadis CP/CPS. In the event that

production of the information

x
  include but do not limit QuoVadis to operating in compliance with:
  - x   documented operational procedures; and
  - x   within applicable law and regulation;
- x   approving the establishment of all Issuing CAs and on approval, executing an Issuing CA Agreement (save in respect of the QuoVadis Issuing CA);
- x   maintaining this

x   If the Digital Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or Organisation;

x   If the Digital Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;

x   If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this QuoVadis CP/CPS and/or the relevant Certificate Holder Agreement or any applicable law or regulation;

x   If the Private Key associated with the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised; or

x   If the Digital Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation.

x   Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided th

x   periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;

x   periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks; and

x   periodically testing uninterrupted power supplies.

9.8.5.   Claims Against QuoVadis Liability
9.8.5.1.   Notification Period
QuoVadis shall have no obligation pursuant to any claim for breach of its obligations hereunder unless the claiming party gives notice to QuoVadis within ninety (90) days after the claiming party knew or ought reasonably to have known of a claim, and in no event more than three years after the expiration of the Digital Certificate held by the claiming party.

9.8.5.2.   Mitigating Acts And Disclosure Of Supporting Information
CP/CPS, a claiming party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such further agreements, instruments, and documents as QuoVadis may reasonably request in order to investigate a claim of loss made by a claiming party.

9.9.   Indemnities
Indemnity provisions and obligations are contained within relevant contractual documentation.

9.10.   Term And Termination
9.10.1.   Term
This CP/CPS becomes effective upon publication in the QuoVadis Repository. Amendments to this CP/CPS become effective upon publication in the QuoVadis Repository.

9.10.2.   Termination
This CP/CPS shall remain in force until it is amended or replaced by a new version.

9.10.3.   Effect Of Termination And Survival
The provisions of this QuoVadis CP/CPS shall survive the termination or withdrawal of a Certificate Holder or Relying Party from the QuoVadis PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the QuoVadis PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

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

9.12.   Amendments
9.12.1.   Procedure Fo6 1 180.62 504.43 Tm[ )]Tri25(i)Tm[)-46(El)3(e)6(c)-5(tro)-2(nic)-4(0 0 1 103.34 232.85 Tm8

10.1.2.   Key Usage and Archive

Different QuoVadis Certificate

10.3.   QV Advanced

PURPOSE

applications including digital signatures, encryption, and authentication.

REGISTRATION PROCESS

Validation procedures for QuoVadis Advanced Digital Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI TS 102 042. Advanced validation is intended to provide equivalent quality to the QCP policy specified in ETSI TS 101 456 but without the legal constraints of the Electronic Signatures Directive (1999/93/EC).

Unless the Certificate Holder has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Certificate Holder shall include the following:

physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence.

Evidence shall be provided of:
- x   Full name (including surname and given names consistent with applicable law and national identification practices); and
- x   Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name

10.4.1.   EIDI-V/ GeBüV Certificates

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

PURPOSE
The EIDI-V/GeBüV Certificate is issued to organisations (companies, municipalities, etc.) and issued primarily to digitally sign electronic invoices. The Certificates may also be used for commercial purposes (such as legally-compliant electronic archiving according to GeBüV).

Organisation (O)	Organisation legal name	Holder Variable
Locality	Locality	Holder Variable
State/Province	State/Province	Holder Variable
Country	Country	Holder Variable
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Non Repudiation	Fixed
Certificate Policies		
CertPolicyID (SuisseID)	2.16.756.5.26.1.1.1	Fixed
User Notice	SuisseID qualified certificate	Fixed
CertPolicyID (Public + SSCD)	0.4.0.1456.1.1	Fixed
CertPolicyID (QuoVadis Cert Class)	1.3.6.1.4.1.8024.1.400	Fixed
URL	http://www.quovadisglobal.com/repository	Fixed
Subject Alternative Name		
RFC822 email address	RFC822 email address (same as subject email address)	Holder Variable

10.5.6   Qualified Certificate Profile ±Organisation ±QCP Public
Please note that where a Qualified Organisation Digital Certificate is issued within the meaning of EU Directive

10.6.   QV Closed Community
Closed Community Issuing CAs can, under contract, create Certificate Profiles for the issuance of Certificates to members of that community.

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 CP/CPS to its community issue various Certificates in accordance with the CP/CPS.

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

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

10.6.1. Grid Certificates
This section provides an overview of the requirements and Digital Certificate contents for Grid Digital Certificates issued in accordance with the requirements of the International Grid Trust Federation (IGTF) or one of its member bodies. The IGTF is the body that is responsible for establishing common policies and guidelines between its member Policy Management Authorities (PMAs). The IGTF consists of the Asia Pacific Grid Policy Management Authority (APGridPMA), the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) and The Americas Grid Policy Management Authority (TAGPMA).

This section (10.6.1) of the CP/CPS relates only to Grid Certificates, which may only be used for Grid related purposes. In relation to Grid Certificates, this section of the CP/CPS will take precedence over the remainder of the CP/CPS if there are any conflicts or contradictions. Major changes to this CP/CPS relating to Grid Digital Certificates will be announced to the relevant Grid PMA and their approval must be gained before Grid Digital Certificates under the new CP/CPS are issued.

All Grid End User Certificates and Grid Server Certificates issued must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125. The QuoVadis Root Certificates are available on the QuoVadis website and also on the TACAR (TERENA Academic CA Repository) trust anchor repository (https://www.tacar.org/repos/).

All Grid Digital Certificates will be issued to Applicants based on cryptographic data generated by the Applicant, or based on cryptographic data that can be held only by the Applicant on a secure hardware token. Any single subject Distinguished Name must be linked to one and only one entity and must not be linked to any other entity over the life of the CA. Pseudonyms will not be allowed for Grid Certificates. Private Key archival or escrow is forbidden for all Grid Digital Certificates.   Revocation requests must be properly authenticated

10.6.1.1.   Grid End User Certificate

PURPOSE

Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid End User Certificate is to help the Certificate Holder to access the Grid services that require

10.6.1.2.	Grid Server Certificate

PURPOSE
Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid Server Certificate is to help secure communications with Grid servers.
REGISTRATION PROCESS

10.7.   QuoVadis Device

PURPOSE

QuoVadis verifies that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. QuoVadis verifies that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by

High Risk Domains

QuoVadis maintains a list of High Risk Domains and has implemented technical controls to prevent the issuance of Certificates to certain domains. QuoVadis follows documented procedures that identify and require additional verification activity for High Risk Certificate Requests pri

FIELDS	CONTENT	DEMARCATION
Subject		
Common Name (CN)	Subject Common Name	Holder Variable
Organisational Unit (OU)	Variable Data	Holder Variable
Organisation (O)	Organisation legal name	Holder Variable

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   Individual or Organisation that has submitted an application for the issue of a Digital Certificate.

Application Software Vendors   developers of Internet browser software or other software that displays or uses certificates and distribute Root Certificates embedded in their software, including but not limited to KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, Red Hat Inc., Adobe, etc.

Approved Client Issuing CA   an Issuing CA managed and operated by an external third party.

Authorised Relying Party
authorizing that person or Organisation to exercise Reasonable Reliance on Digital Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

Authentication
applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to

Certification
the Digital Certificate.

Certification Authority
Certificates.

Certification Authority Officer   , in a trusted role, who is involved in the day-to-day operations of a Certification Authority.

CP/ CPS ´is a publicly available document that details the QuoVadis PKI and describes the practices employed in issuing Digital Certificates.

Certificate Holder
without limitation, organisations, individuals and/or hardware and/or software devices. A Certificate Holder is (i) named in a Digital Certificate or responsible for the Device named in a Digital Certificate and (ii) holds a Private Key corresponding to the Public Key listed in that Digital Certificate.

Operational Term
terminating on the earlier of (i) the date disclosed in that Digital Certificate or (ii) the date of that Digital Certificate Revocation.

Organisation
corporate or un-incorporate, partnership, trust, non-profit making Organisation, or Government entity).

Participants   dis PKI and include (i) Issuing CAs and their Subsidiaries and Holding Companies; (ii) Registration Authorities and their Subsidiaries and Holding Companies; (iii) Certificate Holders, (including Certificate Applicants); (iv) Authorised Relying Parties.

PKCS   -Key Cryptography Standard.

Policy Management Authority   CP/CPS
amendments and general management.

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

Private Key   to the
person that holds it.

Public Key

Repository
Issuing CAs.

Reserved IP Address   n IPv4 or IPv6 address that the IANA has marked as reserved:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root Certification Authority Certificate means the self-signed Digital Certificate issued to the QuoVadis Root
Certification Authority.

Root Certification Authority   s as the source Certification Authority being a self-signed
Certification Authority that signs Issuing CA Certificates.

Secure Signature Creation Device (SSCD) means a secure hardware container specifically designed to carry and protect
a digital certificate, whi