This is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited, (QuoVadis). It contains an overview of the practices and procedures that QuoVadis employs as a Certification Authority (CA). This document is not intended to create contractual relationships between QuoVadis Limited and any other person. Any person seeking to rely on Digital Certificates or participate within the QuoVadis Public Key Infrastructure (the QuoVadis PKI) must do so pursuant to a definitive contractual document. This document is intended for use only in connection with QuoVadis and its business. This version of the CP/CPS has been approved for use by the QuoVadis Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA and as otherwise set out herein. The date on which this version of the CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

This document covers aspects of the QuoVadis PKI that relate to all CAs established by QuoVadis under the QuoVadis Root Certification Authority and the QuoVadis Root Certification Authority 3 (QuoVadis Root CA 3). There are a number of instances where the legal and regulatory framework regarding the issuance of Qualified Certificates under the Swiss, Dutch or European Digital Signature regimes require deviation from QuoVadis standard practices. In these instances, this Document shows these differences either by iQGLFDWLQJ LQ WKH ERG\ RI WKH WH[W ³)RU 4XDO
the inclusion of a Text Box as follows:

	This flag denotes a provision relating to Qualified Certificates issued in accordance with Swiss regulations.
	This flag denotes a provision relating to Qualified Certificates issued in accordance with Dutch regulations.
	This flag denotes a provision relating to Qualified Certificates issued in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures
	This flag denotes a provision relating to Qualified Certificates issued in accordance with Belgian regulations.

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11
Bermuda
Website: http://

Mailing Address:
QuoVadis Limited
Suite 1640
48 Par-La-Ville Road
Hamilton HM-11
Bermuda

QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	WebTrust Revisions
QuoVadis PMA	01 April 2004	2.07	WebTrust Revisions
QuoVadis PMA	11 November 2005	2.08	WebTrust Revisions
QuoVadis PMA	17 April 2006	4.00	Cumulative ZertES Revisions
QuoVadis PMA	14 September 2006	4.1	EIDI-V Certificate Requirements
QuoVadis PMA	26 February 2007	4.2	QuoVadis Root CA 3 Added
QuoVadis PMA	03 April 2007	4.3	Clarifications to Appendix A
QuoVadis PMA	29 October 2007	4.4	General Edits and RFC3647 Conformity, Cumulative ZertES and EIDI-V Revisions
QuoVadis PMA	27 May 2008	4.5	Addition for QV EU Qualified ICA

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.

Where applicable, QuoVadis conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-7UXVWHG &HUWLILFDWHV ³%DVHOLQH 5HTXLUHPHQWV´ SXEOLVK http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The Private Enterprise Object Identifier (OID) assigned by the Internet Assigned Numbers Authority to QuoVadis is 1.3.6.1.4.1.8024.

The Object Identifiers assigned to the Root CAs covered by this CP/CPS are:

x QuoVadis Root Certification Authority/QuoVadis Root CA 1 G3	1.3.6.1.4.1.8024.0.1
x QuoVadis Root CA 3/QuoVadis Root CA 3 G3	1.3.6.1.4.1.8024.0.3

QuoVadis Root CA 2 is used to issue Extended Validation (EV) SSL Certificates associated with EV OID 1.3.6.1.4.1.8024.0.2.100.1.2, Business SSL Certificates and also Code Signing Certificates. Digital Certificates issued under Root CA 2 and QuoVadis Root CA 2 G3 have their own CP/CPS.

This CP/CPS outlines the roles and responsibilities of all parties involved in the generation and use of Digital Certificates and the operation of all QuoVadis-approved:

x Issuing CA services.
x Registration Authority services.

QuoVadis, in its capacity as the Certification Authority, holds the QuoVadis Root Certificates. The QuoVadis Root CA represents the apex of the QuoVadis PKI. The QuoVadis Root CA digitally creates, signs and issues Issuing CA Certificates using one of the Root Certificates identified above. Issuing CA Certificates are only issued to Approved Issuing CAs. An Approved Issuing CA utilises its Issuing CA Certificate to create, sign and issue Digital Certificates.

QuoVadis Issuing CAs are subordinate services that are:

x managed and operated by QuoVadis; or
x managed by third party Organisations but operated by QuoVadis (outsourced services).

Approved Client Issuing CAs are subordinate services that are managed and operated by clients (external services) and meet the contractual, audit and policy requirements of the QuoVadis CP/CPS with regard to operational practices and technical implementation.

Approved Registration Authorities act as the interface between Issuing CAs and an Applicant for a Digital Certificate. Approved RAs perform due diligence on potential Certificate Holder

The diagram below illustrates the components of the QuoVadis PKI:

QuoVadis provides identification and authentication services for 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 S

	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 QuoVadis ³FKDLQ RI WUXVW´

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, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.

x Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.

x Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information

The QuoVadis PMA determines the suitability of this CP/CPS to the functions and uses of Participants in the QuoVadis PKI.

This CP/CPS is regularly reviewed and approved by the QuoVadis PMA. Notice of proposed changes are recorded in the change log at the beginning of this CP/CPS until they are approved, at which time the approved change will be recorded there permanently. Any changes to this CP/CPS that relate to Grid topics (refer to section 10.6.1 below) must be approved by the relevant Grid PMA.

This CP/CPS is published electronically in PDF format at http://www.quovadisglobal.com/repository.

Newly approved versions of this CP/CPS, Certificate Holder or Relying Party Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those documents. Information about amendments to this CP/CPS may be found in Section 9.12.

QuoVadis internal documents not published at http://www.quovadisglobal.com/repository are available only to

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 SubjatET5(o)-3(mp)6(li)5(6( )139.)] TJE-bjat(is)8(tin126(fo)-l5(o)-ltin124-12t)7((d)-( )-(is)-4ltin124-CBT)-14((ti)-9(o)-3(n)-7fo)-5(

Registration information provided by an Organisation may be validated by reference to official government records and/or information provided by a reputable vendor of corporate information services. The accuracy and currency of such information may be validated by conducting checks with financial institution references, credit reporting agencies, trade associations, and other entities that have continuous and ongoing relationships with the Organisation under review. In addition, the telephone number provided by the Organisation as the telephone number of its principal place of business may be called to ensure that the number is active and answered by the Organisation.

Where an Issuing CA or Registration Authority has a separate and pre-existing commercial relationship with the Organisation under review, the Issuing CA or Registration Authority may Authenticate the Identity of the Organisation by reference to records kept in the ordinary course of business that, at a minimum, satisfy the requirements of this section. In all such cases, the Issuing CA or Registration Authority shall record the specific records upon which it relied for this purpose.

	For Qualified Certificates, in accordance with Swiss Digital Signature law, Certificates are only issued to natural persons. These persons may have an affiliation to an organisation which is verified by appropriate documentation.

For Qualified Certificates, in accordance with European/ Dutch/ Belgian Digital Signature law, Certificates are issued to authenticate a person who acts on their own behalf or on behalf of the natural person, legal person or entity they represent. s, in th30.62 72.6 rJET12(e)6(p)6(r)-12(e)6(s)0 0 1

Doc73305(558.7-m15-(34)T7(rt4f)h3(r)-1-61(this)-5( )] TJET213.0513493>>113.54P6(sKI602.38 Tm[(C)] TJET6T13493>>113.54)-61(this)-5( )] TJETBT49134

QuoVadis may provide interoperation services to certify a non-QuoVadis CA, allowing it to interoperate with the QuoVadis PKI. In order for such interoperation services to be provided the following criteria must be met:

x QuoVadis will perform due diligence on the CA;
x A formal contract must be entered into with QuoVadis, which includes a µULJKW WR DXGLW¶ FODXVH and
x The CA must operate under a CPS that meets QuoVadis requirements.

QuoVadis does not support Certificate Renewal. Key Pairs must always expire at the same time as the associated Digital Certificate. Certificate Renewal requests are treated in the same manner as an initial Certificate Request and a new Digital Certificate and new Key Pair is issued. Application for a Digital Certificate following revocation is treated as though the person requesting the replacement were a new Applicant.

Identification and Authentication for routine Re-Key is based on the same requirements as issuance of new Certificates.

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

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

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.

A Registration Authority may request the revocation of Digital Certificates it has caused to be issued by requesting, in

the QuoVadis Root Certification Authority, the QuoVadis Root Certification Authority issues the Issuing CA Digital Certificate to the relevant Issuing CA.

Upon accepting the terms

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

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.

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

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 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.

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.

    Of a change in the employment relationship with the Certificate Holder
    - The Certificate Holder is no longer authorised to act on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
    - The Certificate Holder otherwise becomes unsuitable or unauthorised to hold a Digital Certificate on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
- Affiliation change
- Cessation of operation
- Incorrect information contained in Digital Certificate
- Certificate Holder bankruptcy
- Certificate Holder liquidation
- Certificate Holder death
- Certificate Holder request
- Issuing Registration Authority Request
- Breach of Certificate Holder agreement with QuoVadis

In the event that an Issuing CA determines that its Digital Certificates or the QuoVadis PKI could become compromised and that revocation of Digital Certificates is in the interests of the PKI, following remedial action, QuoVadis will authorise the reissue of Digital Certificates to Holders at no charge, unless the actions of the Holders were in breach of the QuoVadis CP/CPS or other contractual documents.

The following entities may request revocation of a Digital Certificate:

- QuoVadis may revoke any Digital Certificate issued within the QuoVadis PKI at its sole discretion, and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.
- An Issuing CA operating within the QuoVadis PKI may revoke Digital Certificates that it has issued.
- A Registration Authority or Subscriber operating within the QuoVadis PKI may request revocation of Digital Certificates that it requested to be issued.
- Certificate Holders within the QuoVadis PKI may request revocation of their own Digital Certificates.
- 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.

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 Certificate Holder may be required to submit the revocation request via the QuoVadis Support Line or directly over an Internet connection. The QuoVadis website (http://www.quovadisglobal.com) provides a mechanism in which to submit revocation requests. The 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.

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.

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

Revoking a Digital Certificate.

QuoVadis provides optional Key Archive services for certain Certificate Profiles (see Appendix A, section 10.1.2). 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.

Registration Authorities are permitted to instruct QuoVadis to archive the &HUWLILFDWH +ROGHU¶V Private Key for certain Certificate Profiles as specified in their Registration Authority Agreement. End-user Certificate Holder Private Keys shall only be recovered under the circumstances permitted within the Registration Authority Agreement and Trust/Link Administrator Guide.

Archived Private Keys are stored in encrypted form using the QuoVadis Trust/Link application. Certificate Holders are notified when their Private Keys are archived.

Properly authenticated Certificate Holders may subsequently retrieve their own Private Keys.

In addition, properly authenticated RA Officers with specific Key Recovery permissions may request retrieval of a &HUWLILFDWH +ROGHU¶V Private Keys under the following conditions:

‡ 5$V PXVW SURWHFW &HUWLILFDWH +ROGHU¶V DUFKLYHG Private Keys from unauthorized disclosure.

‡ 5$V PD\ UHWULHYH &HUWLILFDWH +ROGHU¶V DUFKLYHG Private Keys only for properly authenticated and authorized requests for recovery.

‡

QuoVadis provides its personnel with on-the-job and professional training in order to maintain appropriate and required

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI.

Only certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction.

All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

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.

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.

QuoVadis supports time stamping of its records. All events that are recorded within the QuoVadis Service include the date and time of when the event took place. This date and time are based on the system time on which the CA system is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis PKI rely on a trusted time source.

The QuoVadis Archive Collection System is internal. QuoVadis provides assistance to Issuing CAs and Registration Authorities within the QuoVadis PKI to preserve their audit trails.

Only specific QuoVadis Trusted Rolesauditors 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 authorised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

Key changeover is not automatic,

When it is necessary to terminate an Issuing CA or Registration Authority service, the impact of the termination will be minimised as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements.

QuoVadis and each Issuing CA specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations. The procedures must, at a minimum:

x ensure that any disruption caused by the termination of an Issuing CA is minimised;
x ensure that archived records of the Issuing CA are retained;
x ensure that prompt notification of termination is provided to Certificate Holders, Authorised Relying Parties, and other relevant parties in the QuoVadis PKI;
x ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained; and
x notify relevant Government and Certification bodies under applicable laws and related regulations.

	For Qualified Certificates, in accordance with Swiss Digital Signature law, a notice of termination of the Issuing CA must be communicated in accordance with pre-established procedures to SAS, the body responsible for accrediting the Certificate Service Provider.
	For Qualified Certificates, in accordance with European/ Dutch/ Belgian Digital Signature law, QuoVadis has implemented procedures to be followed in the event of termination of the service provision. These procedures provide for the transfer of relevant records to a regulatory body and the continuation of revocation status in the event of termination. QuoVadis also has formally documented complaint and dispute resolution procedures.

Where practical, Key and Digital Certificate revocation should be timed to coincide with the progressive and planned rollout of new Keys and Digital Certificates by a successor Issuing CA.

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations and duties as the terminating Issuing CA. The successor Issuing CA should issue new Keys and Digital Certificates to all subordinate service providers and Users whose Keys and Digital Certificates were revoked by the terminating Issuing CA due to its termination, subject to the individual service provider or User making an application for a new Digital Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or Certificate Holder Agreement.

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 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.

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.

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.

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

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

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.

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

A 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.

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 XVH KDUGZDUH &U\SWRJUDSKLF 0RGXOHV VKRXOG EH UHPRYHG DQG VWRUHG
Issuing CA Private Key

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

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

The QuoVadis Time-stamping Authority uses PKI

the QuoVadis PKI. The obligations of Issuing CAs and Registration Authorities within the QuoVadis PKI is established by contract between those entities.

The audit services described in Section 8.1.1 are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and are experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies. The Bermuda Certificate Service Provider and WebTrust audits have been carried out by Ernst & Young. The accreditation audits for Swiss and European signature requirements have been performed by KPMG AG.

The auditor and the Issuing CA under audit, must not have any other relationship that would impair WKH DXGLWRU¶V 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.

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.

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.

If irregularities are found, the Issuing CA in question must submit a report to the QuoVadis Root CA detailing actions the Issuing CA will take in response to the irregularity.

Where the Issuing CA fails to take appropriate action in response to an irregularity, the QuoVadis Root CA may (i) indicate the irregularities, but allow the Issuing CA to continue operations for a limited period of time; (ii) allow the Issuing CA to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation of that Issuing CA¶V ,VVXLQJ &HUWLILFDWH LLL OLPLW WKH FODVV RI DQ\ 'L
CA; or (iv) revoke the Issuing CA's Issuing Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary cessation of the Issuing CA¶V VHUYLFHV EXW DOO UHOHYDQW IDFWRUV PXVW EH FRQVLGHUHG SULRU W
to confirm the implementation and effectiveness of any remedy.

In circumstances where any irregularities are found with FODVVssutT1 0 0 1e I-9(y)5(,)-3(o)-3(t)] TJETBT1 0 0 1 8( )-86(R)-6(to)-2(9

QuoVadis discharges its obligations by:

x providing the operational infrastructure and certification services, including X.500 Directory and service provider software;

x PDNLQJ UHDVRQDEOH HIIRUWV WR HQVXUH LW FRQGXFWV DQ HIILFLHQW D 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 CP/CPS and enforcing the practices described within it and in all relevant collateral documentation;

x publishing its QuoVadis CA Certificates at http://www.quovadisglobal.com/repository and other nominated web sites;

x issuing CA Certificates to Issuing CAs that comply with X.509 standards and are suitable for the purpose required;

x issuing CA

Certificate Holders represent and warrant that:

x The Private Key is protected and has never been accessed by another person.
x All representations made by the Certificate Holder in the Digital Certificate Application are true.
x All information in the Digital Certificate is true and accurate.
x The Digital Certificate is being used for its intended, authorised and legal purpose consistent with this CP/CPS.
x 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.

Relying Parties represent and warrant that:

x 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.
x That they are solely responsible for making the decision to rely on a Digital Certificate.
x 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.

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.

To the extent permitted by applicable law, this CP/CPS, the 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 VKDOO GLVFODLP 4XR9DGLV¶ SRVVLEOH ZDUUDQWLHV LQFOXG 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.

QuoVadis shall be liable to 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) 7KH 'XWFK HOHFWURQLF VLJQDWXUH UHJXODWLRQ ³%HVO ´ $UWLFOH RI ³European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ´

For Qualified Certificates, in accordance with the European/Belgian Digital Signature law, QuoVadis is liable under:

The Belgian Law of 20 October 2000 and the Belgian Law of 9 July 2001

$UWLFOH RI ³European Directive 1999/93/EC of the European Parliament and of the Council of 13

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 that QuoVadis uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;

x Power failure, power interruption, or other disturbances to electrical power, provided QuoVadis uses commercially reasonable methods to protect against such disturbances;

x Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of QuoVadis and/or its subcontractors or service providers; or

x One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which QuoVadis is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of QuoVadis.

Without prejudice to any other provision of this Section 9 4XR9DGLV¶ OLDELOLW\ IRU EUHDFK RI LWV this QuoVadis CP/CPS shall, absent fraud or wilful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below.

Advanced Certificates	US $250,000
Device Certificate	US $250,000
SuisseID Identity and Authentication (IAC) Certificates	CHF 10,000

,Q QR HYAV>•YFEy À`¶ OLDELOHE IRDÀ p3 IRU E> L0I Üð @lute0003>1>>F056>4<06<0003>922()-6te0003>1>>

The only changes that may be made to this CP/CPS without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the QuoVadis PMA, materially impact any Participants within the QuoVadis PKI.

Issuing CAs are notified of changes to the CP/CPS as and when they are approved.

New or amended CP/CPSs are published on the web site at http://www.quovadisglobal.com/repository.

Any change that increases the level of trust* that can be placed in Digital Certificates issued under this CP/CPS or under policies that make reference to this CP/CPS requires thirty (30) days prior notice. Any change that decreases the level of trust that can be placed in Digital Certificates issued under this CP/CPS or under policies that make reference to this CP/CPS requires forty-five (45) days prior notice. The QuoVadis CP/CPS applicable to any Digital Certificate supported by this CP/CPS shall be the QuoVadis CP/CPS currently in effect.

* NOTE: In this section, "level of trust" does not include those parts of the specification relating to the liabilities of the parties. Reference to "level of trust" applies solely to the technical/administrative functions and any changes provided for under this clause shall not materially change this specification unless there is a significant business reason to do so.

The QuoVadis Policy Management Authority reserves the right to amend this CP/CPS without notification for amendments that are not material, including corrections of typographical errors, changes to URLs and changes to contact details. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the QuoVadis Policy Management Authority. Unless the QuoVadis Policy Management Authority determines otherwise, the Object Identifier to this CP/CPS shall not change.

Any controversy or claim between two or more Participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a “Participant” within the QuoVadis PKI) arising out of or relating to this QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

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

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 Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.
- Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

	For Qualified Certificates, in accordance with the Swiss Digital Signature law, all disputes shall be dealt with under Swiss Law.

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.

Procedures for Certificate Holder registration as well as descriptions of fields are described below for each type of Digital Certificate issued. Additionally, specific Certificate Policies and QuoVadis ¶iability arrangements that are not described in this CP/CPS may be drawn up under contract for individual Subscribers.

[redacted]
QV Standard

Different QuoVadis Certificate Profiles may be issued with different key usages, and be eligible for key archive, according to the following table:

[redacted]	[redacted]
Signing and Encryption	digitalSignature nonRepudiation keyEncipherment smartcardlogon c1onRepudnonRepuc

no76.1091 509.6 67.434 m 0 g [(no)-5391.03D 0 0 1 127.Tm 0 g [( )] TJ ET Q g 145.83 509.6 85323e935g [(no76.1091 509.6 67.434 m 0 g [7>> BI

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
Subject Alternative Name	Principle Name = Email Address	Holder Variable
Certificate Policies	This extension includes the QV Advanced + Certificate Class OID = 1.3.6.1.4.1.8024.1.300.	Fixed
Adobe OIDs	Note these Adobe OIDs are only relevant for signing Certificates.	
Adobe Time Stamp (OID = 1.2.840.113583.1.1.9.1)	http://tsa01.quovadisglobal.com/TSS/HttpTspServer	Fixed
Adobe Archive RevInfo (OID = 1.2.840.113583.1.1.9.2)	This relates to OCSP revocation checking within Adobe products for long term validation purposes.	Fixed

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

The ElDI-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).		
These Digital Certificates are issued in accordance with ElDI-V (SR 641.201.1 and SR 641.201.1.1). Validation of these Certificates is performed in accordance with the validation procedures for QuoVadis Qualified Certificates and any additional validation requirements required by ElDI-V.		
Common Name (CN)	Commercial Subject Name or First Name - Last Name	Holder Variable
Organisational Unit (OU)	Variable Data	Holder Variable
Organisational Unit (OU)	Accounting Services (OelDI)/Third Party Services (art. 9 OelDI)	Fixed
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Variable Data	Holder Variable
State/Province (ST)	Variable Data	Holder Variable
Country (C)	Variable Data	Holder Variable
Subject Public Key Information	RSA (2048-bit) / System Generated	Fixed
Key Usage	Digital Signature	Fixed
Key Usage	Non Repudiation	Fixed
Certificate Policies	OID = 1.3.6.1.4.1.8024.0.1.0.0.1 (This is the QuoVadis ElDI-V OID)	Fixed
Policy Qualifier User Notice	Gestuetzt auf Art. 2 Abs. 2 ElDI-V; HQ YHUWX GH O¶DUW DO 2HO', YLVWR O¶DUW FSY 2HO', based on art. 2 para. 2 OelDI; SR 641.201.511 / RS 641.201.511 Schweiz/Suisse/Svizzera/Switzerland	Fixed
Certificate Policies	1.3.6.1.4.1.8024.1.300 (This is the QV Advanced + Certificate Class OID)	Fixed
Policy Qualifier CPS	http://www.quovadisglobal.com/repository	
Subject Alternative Name	Commercial register identification number (ASN-1 printableString coded)	Holder Variable
Subject Alternative Name	Email Address (RFC 822 Name)	Holder Variable
Issuer Alternative Name	O=ZertES Recognition Body: KPMG AG	Fixed
Adobe Time Stamp (OID = 1.2.840.113583.1.1.9.1)	http://tsa01.quovadisglobal.com/TSS/HttpTspServer	Fixed
Adobe Archive RevInfo (OID = 1.2.840.113583.1.1.9.2)	This relates to OCSP revocation checking within Adobe products for long term validation purposes.	Fixed

[redacted]

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Identity and Authentication (IAC) Certificates help provide strong and secure authentication to applications.

Either a Common Name or a Pseudonym is required for a QuoVadis SuisseID IAC Certificate. Use of both Common Name and Pseudonym in the same Certificate is not permitted.

[redacted]

QuoVadis SuisseID IAC Certificates are issued in accordance with the SuisseID requirements (including the ³6XLVVH,' 6SHFLILFDWLRQ´ GRFXPHQW 8QOHVV VWDWHG RWKHUZL in TAV-ZERTES apply to the specification of QuoVadis SuisseID IAC Certificates.

For the issuance and life cycle management of SuisseID IAC Certificates, QuoVadis adheres to the same organizational and operational procedures and uses the same technical infrastructure as for a ZertES compliant qualified certificate.

(YLGHQFH RI WKH &HUWLILFDWH +ROGHU¶V LGHQWLW\ VKDOO EH F have been checked indirectly using means which provide equivalent assurance to physical presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

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

If the Certificate Holder is identified in

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.

[redacted]

[redacted]

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/

Organisation (O)	Organisation legal name	Holder Variable
Locality	Locality	Holder Variable
State/Province	State/Province	Holder Variable
Country	Country	Holder Variable

Please note that where a Qualified

[redacted]

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 Certificate-based authentication.

[redacted]

QuoVadis Device Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. QuoVadis Device Certificates (i.e. with the OID 1.3.6.1.4.1.8024.1.600 in Certificate Policies) that have the Server Authentication Extended Key Usage comply with the CA/B Forum Baseline Requirements.

Device Certificates to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the Certificate is actively engaged in doing business;
- That the Subject named in the Certificate complies with applicable laws;
- That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
- 7KDW LW LV ³VDIH´ WR GR EXVLQHVV ZLWK WKH 6XEMHFW QDPHG

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:

³ ´ PHDQV DQ ,QGLYLGXDO RU 2UJDQLVDWLRQ WKDW KDV VXEPLWWHG DQ D Certificate.

³ ´ PHDQ WKRVH 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.

³ ´ PHDQV an Issuing CA managed and operated by an external third party.

³ ´ PHDQV DQ ,QGLYLGXDO RU 2UJDQLVDWLRQ WKDW KDV HQWH into a Relying Party Agreement authorizing that person or Organisation to exercise Reasonable Reliance on Digital Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

³ ´ PHDQV WKH SURFHGXUHV D nd requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to provide against IUDXG LPLWDWLRQ DQG GHFHSWLRQ´ ³$GG WR EH FRQVLVWHQW ZLWK UHVW DQG ³DXWKHQWLFD\

³ ´ PHDQV WKH SURFHVV RI R-14(a)5(t16>6<0044>5<0057004C005100>5<00510nA003>33<( )6(inc049

³ ´ PHDQV SDUWLFLSDQWV LQ WKH 4XR9DGLV 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.

³ ´ PHDQV 3XEOLF-Key Cryptography Standard.

³ ´ PHDQV WKH 4XR9DGLV ERG\ UHVSRQVLEOH IRU approving CP/CPS RYHUVH amendments and general management.

³ ´ PHDQV DQ\ SDWHQWV SHQGLQJ RU RWKHUZLVH WUDGH PDUNV V 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.

³ ´ PHDQV D .H\ IRUPLQJ SDUW RI D .H\ 3DLU WKDW LV UHTXLUHG WR EH N that holds it.

³ ´ PHDQV D .H\ IRUPLQJ SDUW RI D .H\ 3DLU WKDW FDQ EH PDGH SXEOLF

³ ´ 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.

³ ´ $ 'LJLWDO &HUWLILFDWH ZKRVH SULPDU\ SXUSRVH LV 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.

³ ´ PHDQV 4XR9DGLV /LPLWHG D %HUPXGD H[HPSWHG FRPSDQ\

³ ´ PHDQV 4XR9DGLV LQ LWV FDSDFLW\ DV DQ ,VVXLQJ CA

³ ´ PHDQV WKH LQIUDVWUXFWXUH used by QuoVadis for the generation, distribution, management and archival of Keys, Digital Certificates and Certificate Revocation Lists and the Repository to which Digital Certificates and Certificate Revocation Lists are to be posted.

³ ´means QuoVadis in its capacity as a Root Certification Authority.

³ ´ PHDQV D 5HJLVWUDWLRQ $XWKRULW\ Issuing CA to operate within the QuoVadis E\ DQ PKI responsible for identification and authentication of Certificate Holders.

³ ´ DQ DJUHHPHQW HQWHUHG LQWR EHWZHHQ DQ ,VVXL CA and a Registration Authority pursuant to which that Registration Authority is to provide its services within the QuoVadis PKI.

³ ´ PHDQV D GLJLWDO LGHQWLILHU LVVXHG E\ DQ ,VVXLQJ CA (including QuoVadis in its capacity as an Issuing CA) in connection with the establishment of a Registration Authority within the QuoVadis PKI.

³ ´means the self-signed Digital Certificate issued to the QuoVadis Root Certification Authority.

³ ´ PHDQV 4XR9DGLV DV WKH VRXUFH Certification Authority being a self-signed Certification Authority that signs Issuing CA Certificates.

means a secure container specifically designed to carry and protect a digital certificate, which meets the following requirements laid down in annex III of Directive 1999/93/EC:

1. Secure signature creation devices must, by appropriate technical and procedural means, ensure at the least that:

(a) the signature creation-