QUOVADIS ROOT CERTIFICATION AUTHORITY CERTIFICATE POLICY / CERTIFICATION PRACTICE STATEMENT

OID s:	1.3.6.1.4.1.8024.0.1 1.3.6.1.4.1.8024.0.3
Effective Date:	12 July 2012
Version:	4

1. INTRODUCTION

1.1. Overview

This QuoVadis CP/CPSsets out the policies, processes and procedures followed in the generation, issue, use and management of

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

Tht as Policil tldmrdcoajec tae QuoV-9(a)-14beis

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/CPSand in Appendix A define the credentials necessary to establish the identity of an individual or entity.

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

Participants ("Participants") within the QuoVadis PKI include:

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

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

- accommodate the diversity of the community and the scope of applicability within the QuoVadis chain of trust; and
- 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:

- are the minimum requirements necessary to ensure that Certificate Holders and Authorised Relying Parties have a high level of assurance, and that critical functions are provided at appropriate levels of trust; and
- apply to all stakeholders, for the generation, issue, use and management of all Digital Certificates and Key Pairs.

QuoVadis Digital Certificates comply with Internet Standards (x509 v.3) as set out in RFC 5280 (which supersedes RFC 3280)

Applications are as follows: secure electronic mail, retail transactions, IPSEC applications, secure SSL/TLS applications, contract-signing applications, custom e-Commerce applicationsseoC-5Meorlü1jlÙZÑu¦Q˜áÜ êã À Ùs9 ýéˆV¡ ê€Ñ

QuoVadis is obligated to operate the QuoVadis RootCertification Authority, QuoVadis Issuing CAs, and QuoVadis RAs in accordance with this QuoVadis CP/CPSand other relevant operational policies and procedures with respect to the

	For Qualified Certificates, in accordance with Swiss Digital Signature law, Private Keys are generated on secure signature smartcards in the presence of the Certificate Holder. The Certificate Holder is responsible for securing the smartcard with a Personal Identification Number directly on the Secure Signature Creation Device (SSCD).

For Qualified Certificates, in accordance with European/Dutch Signature law, Private Keys are generated on secure signature smartcards in the presence of the Certificate Holder. The Certificate Holder is responsible for securing the smartcard with a Personal Identification Number directly on the Secure Signature Creation Device (SSCD).

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

x Organisational Unit (OU)

x Other information that is permitted as Non-Verified according to the Certificate class or relevant industry standards

	For Qualified Certificates, in accordance with the Swiss Digital Signature law, all Certificate fields and registration information are verified by appropriate documentation.
	For Qualified Certificates, in accordance with the European/Dutch Digital Signature law, all Certificate fields and registration information are verified by appropriate documentation.

3.2.5. Validation Of Authority

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

3.2.6. Criteria For Interoperation

QuoVadis may provide interoperation services to certify a non-QuoVadis CA, allowing it to interoperate with the oi(,)-2(n)-80(e)-8(t) QuoVadis PKI. In

4.2.3. Time To Process Certificate Appl ications

Registration Authorities and Issuing e(: 0e)-2.Q-6(u)-8(t)-e 4elagi

A

x All representations made by the Certificate Holder to QuoVadis regarding the information contained in the Digital Certificate are true;

x All information contained in the Digital Certificate is true t

- QuoVadisCertification Authority key compromise
- Certificate Holder profile creation error
- Key Compromise including unauthorised access or suspected unauthorised access toPrivate Keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyedor suspected destroyed keys or supersededby replacement keys and a new Certificate.
- The Certificate Holder has failed to meet his, her or its obligations under this QuoVadis CP/CPSor any other agreement, regulation, or law that may be in force with respect to that Digit al Certificate;
- The Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the Certificate Holder provided inaccurate, false or misleading information;
- The Private Key corresponding to the Certificate has been used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a user's system without their consent;
- The Certificate Holder is a denied party or prohibited person on a government-issued blacklist, or is operating from a prohibited destination;
- Where a Certificate Holder's employer or company that operates the Nominating Registration Authority, or its respective Subsidiaries, Holding Companies or Counterparties requests revocation because
    - 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

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/CPSor an equivalent method.

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

4.9.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. Issuing CAs will revoke Digital Certificates

5.3.1. Qualifications, Experience, and Clearance Requirements

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

5.3.2. Background Check Procedures

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

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

5.5. Records Archival

5.5.1. Types Of Records Archived

QuoVadis archives, and makes available upon authorised request, documentation related to and subject to the QuoVadis Document Access Policy. For each Digital Certificate, the records contain information related to creation, issuance, intended use, revocation and expiration. These records will include all relevant evidence in the Issuing CA's possession including:

x

5.7. Compromise And Disaster Recovery

QuoVadis has a CAOperations Disaster & Recovery Plan (QuoVadis Business Continuity Plan). The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by fire, strikes, etc.

QuoVadis and each Issuing CA have in place an appropriate disaster recovery and business resumption plan that provides for the immediate continuation of Digital Certificate revocation services in the event of an unexpected emergency. QuoVadis regards its disaster recovery and business resumption plan as proprietary security-sensitive, and confidential. Accordingly, it is not intended to be made generally available.

QuoVadis and each IssuingCA have in place an appropriate Key compromise plan detailing the activities taken in the event of a compromise of a QuoVadis Issuing CA A re 633K4m6(o)31(i-5t)7E2010)]TJ 4(d)-6(8)-0JTHmyAataa10Tc10.12 T1)]T 1.0093 8w61.2 u 7.71(e)4(r)-'(h)-s(Tc 0.12 Tww 0.453 66Td [(a)2 Te)4(r)-P.1

5.8.2. Successor Issuing Certification Authority

To the extent that it is prac tical and reasonable, the successor Issuing CA should assume the same rights, obligations and duties as the terminating Issuing CA. The successor Issuing CAshould 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 Identifica tion 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/sm artcards 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 te2am holds total(h7E2t0.12 Tw -7.2i0 Td (3)Tj 0.56 0 Tds)1-10(nnt)]TJ 0 Tc 0ti14gemhe3oemeam0 Tc 0heuoemet lcu3 AuHuoldare se

6.1.4. Certification Authority Public Key To Relying Parties

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

6.1.5. Key Sizes

Key lengths within the QuoVadis PKI are determined by Certificate Profiles more fully disclosed in Appendix A. The QuoVadis Issuing CAs use an RSA minimum [illegible]

6.2.4. Private Key Backup

All Issuing CA Keys are held in secure cryptographic devices and are equally secured whenever stored outside the FIPS-boundary of the secure cryptographic device, never appearing in plaintext. Issuing CA Private Keys are stored in an encrypted state (using an encryption key to create a "cryptographic wrapper" around the key). Access is only 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 E

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:

- Access controls to Certificate Authority services and PKI roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and PKI roles, see Section 5.2
- Identification and Authentication of personnel that fulfil role s of responsibility in the QuoVadis PKI, see Section 5.3
- Use of cryptography for session communication and database security, mutually authenticated and encrypted SSL/TLS is used for all communications
- Archival of Certificate Authority history and audit da ta, see Sections 5.4 and 5.6
- 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 s oftware 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 n ew 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 ongoingioasgi(n)-8Tw 30 0s mf()-12(.)-10(5)-7

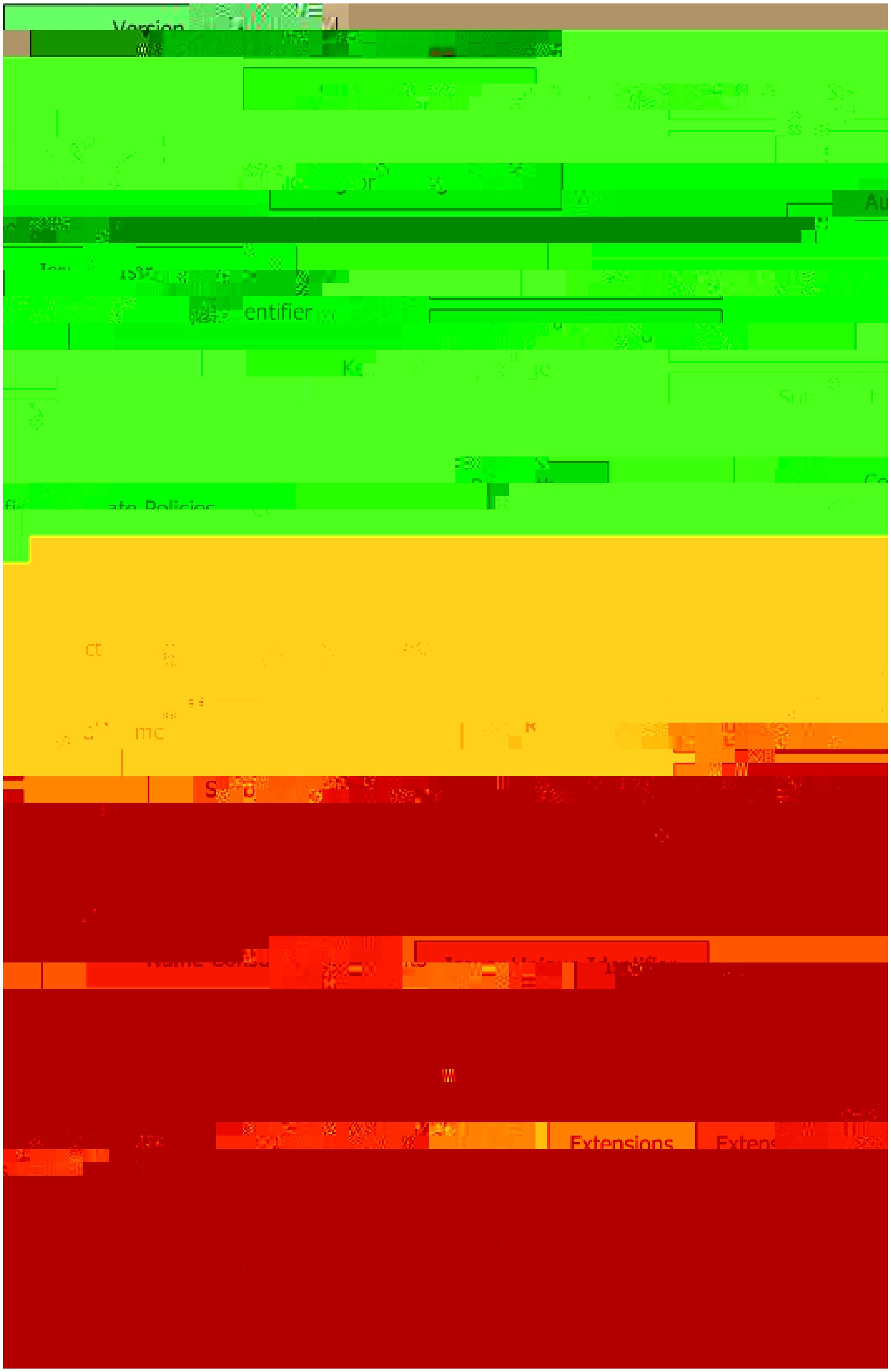
7.1.1. Basic Certificate Contents

FIELDS	CONTENT	DEMARCATION
Version	The version of the encoded certificate. QuoVadis certificates are Version 3	Fixed
Serial Number		

FIELDS	CONTENT	DEMARCATION
Certificate Policies	This extension contains Object Identifiers (OIDS) as well as a URL with a link to the QuoVadis Repository at http://www.quovadisglobal. com/repository. QuoVadis Certificates issued up to and including version 4.6 of this CP/CPS contain the OIDs for QuoVadis Root 1 (1.3.6.1.4.1.8024.0.1) or QuoVadis Root 3 (1.3.6.1.4.1.8024.0.3). QuoVadis Certificates issued from version 4.7 onwards will instead contain an OID that relates to the QuoVadis Certificate Class. Refer to section 10.1.1 for further information in relation to QuoVadis Certificate Classes and the related OIDS.	Fixed
Subject Alternative Name	This extension allows identities to be bound to the subject of the Certificate and can include Internet e- mail address, Microsoft UPN, a DNS name, IP address, or a Uniform Resource Identifier (URI). Refer to Appendix A for the Subject Alternative Name specific to each class of QuoVadis Certificates. All parts of the Subject Alternative Name included in the Digital Certificate will be subject to verification.	Holder Variable
Extended Key Usage (EKU)	This extension indicates one or more purposes for which the certified Public Key	

7.5. Digital Certificate Fields and Root CA Certificate Hashes

7.5.1. Digital Certificate Fields



7.5. 2 QuoVadis Root Certificate Hashes

Note that all QuoVadis CA Certificates and CRLs are available for download from the QuoVadis Repository at http://www.quovadisglobal.com/repository .

7.5.2.1. QuoVadis Root CA Certificate Hashes

Field	Certificate Profile
Serial Number	3ab6508b
Signature Block	Signature matches Public KeyRoot Certificate: Subject matches Issuer Key Id Hash (sha1): 86 26 cb 1b c5 54 b3 9f bd 6b ed 63 7f b9 89 a9 80 f1 f4 8a Subject Key Id (precomputed): 8b 4b 6d ed d3 29 b9 06 19 ec 39 39 a9 f0 97 84 6a cb ef df Cert Hash(sha1): de 3f 40 bd 50 93 d3 9b 6c 60 f6 da bc 07 62 01 00 89 76 c9

7.5.2.2. QuoVadis Root CA 3 Certificate Hashes

Field	Certificate Profile
Serial Number	05c6
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash(sha1): 14 8d b3 54 ed 9b 2f 13 08 7c c3 8b 4b c1 5b 96 8a c5 53 78 Subject Key Id (precomputed): f2 c0 13 e0 82 43 3e fb ee 2f 67 32 96 35 5c db b8 cb 02 d0 Cert Hash(sha1): 1f 49 14 f7 d8 74 95 1d dd ae 02 c0 be fd 3a 2d 82 75 51 85

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	As defined in Bermuda's Electronic Transactions Act 1999, an Authorised Certification Service Provider serves as a trusted third party to help ensure trust and security in support of electronic transactions.
WebTrust for Certification Authorities	The WebTrust Seal of assurance for Certification Authorities (CA) symbolises to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria.
SR 943.03 [ZertES]	Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) Dated: 19 December 2003 Status: 1 August 2008
SR 943.032 [VZertES]	Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES) Dated: 3 December 2004 Status: 1. January 2005
SR 943.032.1 [TAV]	Verordnung des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur Dated: 6 December 2004 Status: 21 November 2006 SR 943.032.1 / Anhang: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur Dated: 13 November 2006 Status: 13 November 2006
ESI ("Directive")	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
ETSI TS 101 456	TS 101 456 EU Standards Body Technical Specification - Policy Requirements for certification authorities issuing qualified Certificates
ETSI TS 101 862	TS 101 862, Qualified Certificate Profile
EUGridPMA	Accredited Certification Authority by the EU Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).
PKI Overheid	Accredited Certification Service Provider

8.1.3. Registration Authorities

Selected Registration Authorities within the QuoVadis PKI are subject to annual compliance reviews performed by or on behalf of QuoVadis in order to determine compliance by those entities with their operational requirements within the QuoVadis PKI. The obligations of Issuing CAs and Registration Authorities within the QuoVadis PKI is established by contract between those entities.

8.2. Identity And Qualifications Of Assessor

The audit services described in Section 8.1.1 are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and 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.

8.3. Assessor's Relationship To Assessed Entity

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

8.4. Topics Covered By Assessment

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

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 law, the course of action and time

	For Qualified Certificates issued in accordance with European/Dutch Digital Signature laws, Certificate Holders expressly consent to personal data in the form of the data included in the Certificate Fields being transferred outside of The Netherlands and published in a repository which makes this information publicly available to persons searching the repository with the appropriate query string. Personal data obtained during the registration process which is not included in the Certificate Fields will not be transmitted outside of The Netherlands.

9.4.6. Disclosure Pursuant To Judicial Or Administ9.4.otcis d6. 1

9.5.3. IETF Guidelines

The use of the PKIX IETF Guidelines is acknowledged.

9.5.4. Breach

QuoVadis excludes all liability for breach of any other intellectual property rights.

9.6. Representations And Warranties

9.6.1. Certification Authority Representations

9.6.1.1 Root Certification Authority Representations

o otoot2439 r-23(4(w 7.4o)()1ief a)-8(y)-ac7(i)-4(g)1ino(oot2()1ie439 re-6(o)-8(o)()1ibl)-17(i5l) TcTJ 0 T2(oot2439 rd-4(i)TJ 0 T(pr)s)thyn

- documented operational procedures; and
- applicable law and regulation.

9.6.2.2 Warranties

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

9.6. 3. Certificate Holder Representations And Warranties

Certificate Holders represent and warrant that:

- The Private Key is protected and has never been accessed by another person.
- All representations made by the Certificate Holder in the Digital Certificate Application are true.
- All information in the Digital Certificate is true and accura te.
- The Digital Certificate is being used for its intended, authorised and legal purpose consistent with this CP/CPS
- They will promptly request revocation of the Digital Certificate in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key listed in the Digital Certificate.

9.6. 4. Relying Parties Representations And Warranties

Relying Parties represent and warrant that:

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

9.6. 5. Representations And Warranties Of Other Participants

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

9.7. Disclaimers Of Warranties

To the extent permitted by applicable law, this CP/CPS, the Certificate Holder Agreement, the

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.

9.12.2. Notification Mechanism And Period

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.

9.12.3. Circumstances Under Which Object Identifiers Must Be Changed

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.

9.13. Dispute Resolution Provisions

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.

9.14. Governing Law

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

x Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.

x Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.

x 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.
	For Qualified Certificates, in accordance with the Dutch Digital Signature law, all disputes shall be dealt with under Dutch Law. For Qualified Certificates issued in other jurisdictions, disputes will be dealt with under the national law of the relevant Member State.

9.15. Compliance With Applicable Law

This CP/CPS is subject to applicable law.

9.16. Miscellaneous Provisions

Not Applicable.

9.16. 1. Entire Agreement

Not Applicable.

9.16. 2. Assignment

Not Applicable.

9.16. 3. Severability

Any provision of this QuoVadis CP/CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this QuoVadis CP/CPS or affecting the validity or enforceability of such remaining provisions.

9.16. 4. Enforcement (Attorneys' Fees And Waiver Of Rights)

The failure or delay of QuoVadis to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by this QuoVadis CP/CPS; shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of this QuoVadis CP/CPS is intended to be exclusive of any other right or remedy, except as expressly provided in this QuoVadis CP/CPS, and each and every right or remedy shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

9.16. 5. Force Majeure

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

9.17. Other Provisions

No Stipulation.

10.1. 2. Key Usage and Archive

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

QuoVadis Certificate Type	Key Usage / Extended Key Usage	Applicability of Certificate Types to QuoVadis Certificate Classes			
		QV Standard	QV Advanced	QV Advanced +	QV Qualified
Signing and Encryption	Key Usage digitalSignature nonRepudiation keyEncipherment Extended Key Usage smartcardlogon clientAuth emailProtection	Allowed (Archival permitted)	Allowed (Archival permitted)	Allowed (Archival not permitted)	Not Allowed
Signing	Key Usage digitalSignature nonRepudiation Extended Key Usage smartcardlogon clientAuth emailProtection	Allowed (Archival not permitted)			

10. 2. QV Standard

PURPOSE
Standard Digital Certificates provide flexibility for a range of uses appropriate to their reliance value including electronic signatures, authentication, and encryption.

REGISTRATION PROCESS
Validation procedures for QuoVadis Standard Digital Certificates collect either direct evidence or an attestation from an appropriate and authorised source, of the identity (such as name and organisational affiliation) and other specific attributes of the Certificate Holder.

FIELDS	CONTENT	DEMARCATION
Subject		
Email Address (E)E)E)		

10.3. QV Advanced

PURPOSE

Advanced Digital Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, encryption, and authentication.

REGISTRATION PROCESS

Validation procedures for QuoVads Advanced Digital Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI TS102 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:

If the Certificate Holder is a physical person, evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence.

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 recognised 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 a physical person who is identified in association with an organizational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organizational entity;
- Any relevant existing registration information (e.g. company registration) of the organizational entity; and
- Evidence that the Certificate Holder is associated with the organizational entity.

If the Certificate Holder is an organizational entity, evidence shall be provided of:

- Full name of the organizational entity; and
- Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

FIELDS	CONTENT	DEMARCATION
Subject		
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	

10.4.2 SuisseID Identity and Authentication Certificate s

PURPOSE
SuisseID is the first standardised electronic proof of identity in Switzerland (http://ww w.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

State/Province	State/Province	Holder Variable
Country	Country	Holder Variable

Extensions		
Key Usage	Digital Signature Non Repudiation	Holder Variable Fixed
Subject Alternative Name	Principal Name = Email Address	Holder Variable
QC Statement PKIX Compliance	1.3.6.1.5.5.7.11.2	Fixed
QC Statement ETSI Compliance	0.4.0.1862.1.1	Fixed

10.5.4. SuisseID Qualified Certificates

PURPOSE

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Qualified Certificates are used to sign documents electonically. The digital signature is tamperproof and legally equivalent to a handwritten signature.

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

REGISTRATION PROCESS

QuoVadis SuisseID Qualified Certificates are issued in accordance with the SuisseID requirements (including the "SuisseID Specification" document). Unless stated otherwise in the SuisseID Specification document, the guidelines in TAV-ZERTES apply to the specification of SuisseID Qualified Certificates.

For the issuance a(e)-i(c)-12S4i<P <</MCIDah-8(c)-12(e)-12(a)-1((afaQ4.4a68(e)13(m)-i(c)-12S4i<e2(do)-1)-4(ssu)-a6868(e)135

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)	

10.6. QV Closed Community

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

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

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

Under no circumstances can Closed Community Issuing CAs issue Qualified CertificAm-17(ed Co)-6(t)nca

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 Certificate-based authentication.
REGISTRATION PROCESS
The identity vetting of all Applicants must be performed by an approved Registration Authority (RA). Face to face registration is required at the RA or alternatively the Applicants can have their identity vetted at a post office providing an approved identity vetting service. The Applicant must present a valid photo ID and/or valid official documents in accordance with formally documented RA procedures. The RA is responsible for recording, at the time of validation, sufficient information regarding the Applicant to identify the Applicant. The RA is responsible for maintaining documented evidence on retaining the same identity over time. The Digital Certificate request submitted for certification must be bound to the act of identity vetting.

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

The identity vetting of all Applicants must be performed by an approved Registration Authority (RA). For Grid Server Certificates, the RA must validate the identity and eligibility of the person in charge of the specific entities using a secure method. The RA is responsible for recording, at the time of validation, sufficient information regarding the Applicant to identify the Applicant.

As part of the registration process the RA must ensure that the Applicant is appropriately authorised by the owner of the associated Fully Qualified Domain Name (FQDN) or the responsible administrator of the machine to use the FQDN identifiers asserted in the Digital Certificate. The RA is responsible for maintaining documented evidence on retaining the same identity over time.

The RA must validate the association of the Certificate Signing Request. The Certificate Request submitted for certification must be bound to the act of identity vetting.

DIGITAL CERTIFICATE DELIVERY

Private Keys pertaining to Grid Server Certificates may be stored without a passphrase, but must be adequately protected by system methods if stored without passphrase.

FIELDS	CONTENT	DEMARCATION
Issuer		
Common Name (CN)	QuoVadis Grid ICA	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Limited	Fixed
Country (C)	BM	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M (Maximum certificate lifetime of 1 year)	Fixed
Subject		
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=< organisation identifier >, DC=hosts	Holder Variable
Common Name (CN)	Subject Common Name	Holder Variable
Organisational Unit (OU)	Optional	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Optional	Holder Variable
State/Province (ST)	Optional	Holder Variable
Country (C)	Optional	Holder Variable
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Extensions		
Key Usage (Critical)	Digital Signature Key Encipherment Data Encipherment	Fixed
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.8024.0.1.10.0.0.4.7 [2]Certificate Policy: Policy Identifier=1.2.840.113612.5.2.2.1 [3]Certificate Policy (QuoVadis Certificate Class OID) Policy Identifier=1.3.6.1.4.1.8024.0.500	Fixed
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Fixed
Authority Information Access	URL=http://trust.quovadisglobal.com/qvgridg1.crt	Fixed
CRL Distribution	http://crl.quovadisglobal.com/qvgridg1.crl	Fixed

"Certificate Revocation List" means a list of Digital Certificates signed by the Issuing Certification Authority that have been revoked.

"Counterparty" means a person that is known to a Nominating Registration Authority or its respective Subsidiaries or Holding Companies and where the relationship with the Counterparty was established in accordance with recognised and documented Know Your Customer standards and with whom the Registration Authority is reliably able to identify the Counterparty through business records maintained by the Registration Authority or obtained from its respective Subsidiaries or Holding Companies.

"Cryptographic Module" means secure software, device or utility that (i) generates Key Pairs; (ii) stores cryptographic information; and/or (iii) performs cryptographic functions.

"Digital Certificate" means a digital identifier within the QuoVadis PKI that: (i) identifies the Issuing CA; (ii) identifies the Holder; (iii) contains the Holder's Public and Private Keys; (iv) specifies the Digital Certificate's

“Operational Term

"Repository" means one or more databases of Digital Certificates and other relevant information maintained by Issuing CAs.

"Reserved IP Address" means an 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" means QuoVadis as the source Certification Authority being a self-signed Certification Authority that signs Issuing CA Certificates.

"Secure Signature Creation Device" (SSCD) 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-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
   (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
   (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory
   against the use of others.
2. Secure signature-