QuoVadis

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

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.

1.4.1. Appropriate Certificate Usage

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

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

A Digital Certificate does not convey evidence of authority of an Individ

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

No reliance may be placed on Digital Certificates and Digital Certificates may not be used in circumstances (i) where

4.2.3. Time To Process Certificate Applications

Registration Authorities and Issuing CAs

Holder (or Organisation, where applicable) may request revocation by contacting the Issuing CA and providing

5.2.1. Trusted Roles

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

Certificate and hardware security lifecycle management is recorded.
Logs recording all network traffic to and from trusted machines are recorded and audited.
All aspects of the configuration of the backup site are recorded. All procedures involved in the backup process are recorded.
All data recorded as mentioned in the above sections is backed up. Therefore, there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios.
All aspects of the installation of new or updated software.
All aspects of hardware updates.
All aspects of shutdowns and restarts.
Time and date of Log Dumps.
Time and date of Transaction Archive Dumps.
Security profile changes
Logins and logouts on servers

All Audit logs will be appropriately time-stamped and their integrity protected.

5.4.2. Frequency Of Processing Log
Audit logs are verified and consolidated at least monthly.

5.4 .3. Retention Period For Audit Log
Audit logs are retained as archive records for a period no less than eleven (11) years for audit trail files, and no less than eleven (11) years for Key and Digital Certificate information. Audit logs are stored until at least eleven

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:

- Audit logs;
- Digital Certificate requests and all related actions;
- Contents of issued Digital Certificates;
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Revocation requests and all related actions;
- Archive and retrieval requests;
- Digital Certificate Revocation Lists posted;
- Audit Opinions as discussed in this QuoVadis CP/CPS; and
- Name of the relevant QuoVadis Registration Authority.

5.5.2. Retention Period For Archive

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

5.5.3. Protection Of Archive

5.7. Compromise And Disaster Recovery

QuoVadis has a CA Operations 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 Issuing CA have in place an appropriate Key compromise plan detailing the activities taken in the event of a compromise of a QuoVadis Issuing QuoV ¶ V aQuoVd

5.8.2. Successor Issuing Certification Authority

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.

6. TECHNICAL SECURITY CONTROLS

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

6.1. Key Pair Generation And Installation

6.1.1. Key Pair Generation

All Key Pairs will be generated in a manner that QuoVadis, in its sole discretion, deems to be secure.

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

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

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

6.1.2. Private Key Delivery To Certificate Holder

In most cases, a Private Key will be generated and remain within the Cryptographic Module. If the owner of the Cryptographic Module generates the Key, then there is no need to deliver the Private 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 electron5(n)-14(d)(Ce)

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 CA uses an RSA minimum key length of 2,048-bit modulus. QuoVadis issuing CAs created after January 1, 2008 use an RSA minimum key length of 4,096-bit modulus.

6.1.6. Public Key Parameters Generation And Quality Checking

For Certificate Holders, the quality of parameters used to create Public Keys are determined by the relevant Registration Authority application or by the & H U W L I L F D W H ¶V client application.

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

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

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

An Issuing & $ ¶V Private Keys may be used for Digital Certificate signing and CRL and OCSP response signing. Keys may also be used to authenticate the Issuing CA to a Repository.

6.2. Private Key Protection And Cryptographic Module Engineering Controls

All Participants in the QuoVadis PKI are required to take all appropriate and adequat3(ta)-7(kI/Top]/Type/ e0c5(ll)5( )-86(a)5(p)6(p)6(ro

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 W R F U H D W H D ³ F U \ S W R ´ Root CA Key). Access to U´ by N-

6.2.11. Cryptographic Module Rating

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

6.7. Network Security Controls

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.

6.8. Time-Stamping

The QuoVadis Time-stamping Authority uses PKI and trusted time sources to provide reliable standards-based time-stamps. The QuoVadis Time-stamp Policy defines the operational and management practices of the QuoVadis Time-stamp Authority such that Participants and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

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

The structure and content of the QuoVadis Time-stamp Policy is in accordance with ETSI TS 101 023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities. The QuoVadis Time-stamp Policy is administered and approved by the QuoVadis Policy Management Authority and should be read in conjunction with this CP/CPS.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

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

The table below describes the basic fields that may be included in QuoVadis Digital Certificates. Refer to APPENDIX A for additional Certificate contents that are specific to the individual classes of Digital Certificates.

7.1.1. Basic Certificate Contents

FIELDS	CONTENT	DEMARCATION
Version	The version of the encoded certificate. QuoVadis certificates are Version 3	Fixed
Serial Number	Unique system generated number assigned to each certificate	Fixed
Signature Al gorithm		

[redacted]

7.5. Digital Certificate Fields and Root CA Certificate Hashes

7.5.1. Digital Certificat e 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

[redacted]

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1.

In circumstances where any irregularities are found with respect to QuoVadis, in its capacity as an Issuing CA, the principles enunciated above will be followed by the QuoVadis Root CA.

8.5.2. Registration Authorities

If irregularities are found, the QuoVadis Root CA, or if applicable the Issuing CA, will address the issues raised with the relevant entity. Any action to be taken wil l be determined by QuoVadis by reference to its determination as to the severity or materiality of the irregularity. In the event that QuoVadis determines that remedial action is required, the relevant entity will be advised by QuoVadis as to the procedures and action required to remedy the irregularity. Remedial action determined by QuoVadis shall be limited to the operations and procedures required to be taken in order to ensure that the Registration Authority operates in compliance with the QuoVadis CP/CPS. In the event that 4XR9DGLV GHWHUPLQHV WKDW UHPHGLDO DFWLRQ LV UHTXLUHG DQG VXFK D determination, QuoVadis may (i) allow the Nominating Issuing CA to continue operations for a further period of time whilst the irregularities are addressed; (ii) allow the Nominating CA and its Registration Authority to continue operations for a maximum of thirty (30) days pending full implementation of the actions required by QuoVadis prior to termination of that Issuing CA¶ RU 5HJLVWUDWLRQ $XWKRULW\ Agreement with QuoVadis and the associated revocation of any Digital Certificate issued to them; (iii) limit the class of any Digital Certificates issued by the Nominating Issuing CA; or (iv) terminate that Issuing CA¶V DJUHHPHQW with QuoVadis and revoke the Issuing &HUWLILFDWH $Q\ GHFLVLRQ UHJDUGLQJ ZKLFK RI WKHVH DFWLRQV WR WDNH and materiality of the irregularities.

8.6. Publication Of Audit Results

The audit opinion based on resul4(c1fit)-9( )-13 Tinuetancesbwillheallncevaivabencupon reqest The tesul4(c1fit)-9( )-13 Tinuetancmoiest

9.2.1. Insurance Coverage

QuoVadis maintains in full force and effect a liability insurance policy. In accordance with the requirement of ZERTES, policy limits concerning Qualified Digital Certificates are maintained in excess of the minimum requirement of CHF 2 (Two) Million per occurrence and CHF 8 (Eight) Million annual aggregate.

Within the QuoVadis PKI the Root CA and all Issuing CAs and Registration Authorities are required to demonstrate that they have the financial resources necessary to discharge their obligations under this CP/CPS and any other relevant and associated documentation or agreements.

QuoVadis and each Issuing CA and/or Registration Authority shall maintain appropriate insurances necessary to provide for their respective liabilities as Participants within the QuoVadis PKI. Failure to establish and maintain insurances may be the basis for the revocation of their respective Digital Certificates.

9.2.2. Other Assets

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

9.2.3. Insurance Or Warranty Coverage For End-Entities

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

QuoVadis Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the Private Key that corresponds to the Public Key in their QuoVadis Digital Certificate.

QuoVadis Relying parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.2.4. Fiduciary Relationships

QuoVadis is not the agent, fiduciary or other representative of any Certificate Holder and/or Relying Party and must not be represented by the Certificate Holder and/or Relying Party to be so. Certificate Holders and/or Relying Parties have no authority to bind QuoVadis by contract or otherwise, to any obligation.

Participation in the QuoVadis PKI does not make any participant an agent, fiduciary, trustee, or other representative of any entity, legal or otherwise. Nothing contained in this QuoVadis CP/CPS or in any corresponding Certificate Holder or Relying Party Agreement shall be deemed to constitute QuoVadis, QuoVadis PKI Participants or any of their agents, directors, employees, consultants, suppliers, contractors, partners or Counterparties a fiduciary, endorser, promoter, agent, partner, representative, or Counterparty of any entity, and the use of or reliance upon Digital Certificates or other forms of participation within the QuoVadis PKI is to be construed accordingly.

9.3. Confidentiality Of Business Information

9.3.1. Scope Of Confidential Information

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

QuoVadis discharges its obligations by:

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

P D N L Q J U H D V R Q D E O H H I I R U W V W R H Q V X U H L W F R Q G X F W V D Q H I I L F L H Q W D

include but do not limit QuoVadis to operating in compliance with:

documented operational procedures; and

within applicable law and regulation;

approving the establishment of all Issuing CAs and on approval, executing an Issuing CA Agreement (save in respect of the QuoVadis Issuing CA);

maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation;

publishing its QuoVadis CA Certificatesat http://www.quovadisglobal.com/repository

documented operational procedures; and
applicable law and regulation.

9.6.2.2 Warranties

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

9.6.3. Certificate Holder Representations And Warranties

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 accurate.
The Digital Certificate is being used for its intended, authorised and legal purpose consistent with this CP/CPS
They will promptly request revoc

9.12.2. Notification Mechanism And Perio d

New or amended CP/CPSs are published on the web site at

9.16. Miscellaneous Provisions

Not Applicable.

9.16. 1. Entire Agreement

Not Applicable.

9.16. 2.

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 keyEnciphermen t 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)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)
Encryption	Key Usage keyEnciphermen t Extended Key Usage emailProtection	Allowed (Archival permitted)	Allowed (Archival permitted)	Allowed (Archival not permitted)	Not Allowed
Authentication	Key Usage digitalSignature Extended Key Usage smartcardlogon clientAuth	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Not Allowed

The Certificate Profiles that follow indicate the fields which are VARIABLE on initial registration by the Certificate + R O G H U ³ + R O G H U 9 D U L D E O H ´ D Q G W K R V Heir based on policy or by IETF Standard, V V X L Q J & $ applicable law, or regulation.

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 affili ation) and other specific attributes of the Certificate Holder. Ema34.42 T Q EMC Orge

FIELDS	CONTENT	DEMARCATION
Subject		
Email Address (E)	43 ET Q EMC Orgerp Q q 0 U 8 0 2 2 6 4 2 5 3 0 6 4 1 3 9 2 2 1 0 8 re41.66 n BT 1 0 0 1 81.024 Tc 66.26 Tw 0 15447ma43J ET Q	

10.4. QV Advanced +

PURPOSE

QuoVadis Advanced+ Digital Certificates are used for the same purposes as QuoVadis Advanced Digital Certificates, with the only difference being that they are issued on a Secure Signature Creation Device (SSCD) that meets the requirements laid down in annex III of Directive 1999/93/EC. The QuoVadis Advanced + Certificate Class is trusted in the Adobe Approved Trust List (AATL).

Enhanced Key Usage	Smart Card Logon (Optional)	Holder Variable
Subject Alternative Name	Principle Name = Email Address	Holder Variable

10.4.2 SuisseID Identity and Authentication Certificates

PURPOSE
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.
REGISTRATION PROCESS
QuoVadis SuisseID IAC Certificates are issued in accordance with the SuisseID requirements (including the ³6XLVVH,'6SHFLILFDWLRQ´GRFXPHQW 8QO Specification Document, the guidelines 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 FKH 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 association with an organisational entity, additional evidence shall be provided of: Full name and legal status of the associated organisational entity; Any relevant existing registration information (e.g. company registration) of the organisational entity; Authorization from an authorized Organisation representative; and Evidence that the Certificate Holder is associated with the organisational entity. QuoVadis SuisseID IAC Certificates must be issued on a SSCD and adhere to the following requirements: SSCD storage, preparation, and distribution is securely controlled by CA or RA; User activation data is securely prepared and distributed separately from the SSCD; 7KH &HUWLILFDWH +RO Private Key can be maintained under the subject's sole control; and 2QO\ XVH WKH &HUWLILFDWH +RO GHU¶V 3ULYDWH .H\ IRU VLJQL QuoVadis SuisseID IAC Certificates have a maximum validity of three years.

FIELDS	CONTENT	DEMARCATION
Issuer		
Common Name (CN)	QuoVadis SuisseID Advanced CA	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink Switzerland Ltd.	Fixed
Country	CH	Fixed
Subject		
Common Name (CN)	First Name - Last Name (Authentication)	Holder Variable
Pseudonym	Pseudonym (Authentication)	Holder Variable
Title	Title (e.g. Dr.) which must be as written in ID Document/ Passport)	Holder Variable
Serial Number	1200-xxxx-xxxx-xxxx	

10.5. QV Qualified

10.5.1. Qualified Certificate Profile

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.

PURPOSE
The purpose of a Qualified Digital Certificate is to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified electronic signatures meeting the qualification requirements defined by the applicable legal framework of the Electronic Signatures Directive (1999/93/EC). The QuoVadis Qualified Certificate Class is trusted in the Adobe Approved Trust List (AATL).

REGISTRATION PROCESS
Validation procedures for QuoVadis Qualified Digital Certificates are consistent with the Qualified Certificate Policy + SSCD (QCP public +SSCD) policy described in ETSI TS 101 456. ,I WKH &HUWLILFDWH +RODHU LV D SK\VLFDO SHUVRQ HYLGHQFH RI 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 organisational entity, additional evidence shall be provided of: Full name and legal status of the associated organisational entity; Any relevant existing registration information (e.g. company registration) of the organisational entity; and Evidence that the Certificate Holder is associated with the organisational entity. QuoVadis Qualified Digital Certificates require a Secure Signature Creation Device (SSCD) that meets the requirements laid down in annex III of Directive 1999/93/EC. SSCD storage,preparation, and distribution is securely controlled by CA or RA; User activation data is securely prepared and distributed separately from the SSCD; ,I NH\V DUH JHQHUDWHG XQGHU WKH &HUWLILFDWH +RODHU¶V signing or decrypting; 7KH &HUWLILFDWH +RODHU¶V Private Key can be maintained under the subject's sole control; and 2QO\ XVH WKH &HUWLILFDWH +RODHU¶V Private Key for signing or decrypting with the SSCD.

FIELDS	CONTENT	DEMARCATION
Subject		
Email Address (E)	aaa@bbb.xx.yy or aaa@bbb.com	Holder Variable
Common Name (CN)	First Name - Last Name	Holder Variable
Organisational Unit (OU)	Qualified Certificate	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Not Stipulated	Holder Variable
State or Province	Not Stipulated	Holder Variable
Country	ISO Country Code	Holder Variable
Date Of Birth	DD/MM/YYYY	Holder Variable
Place of Birth	City	Holder Variable
Gender	M/F	Holder Variable
Title	Verified Legal Title	Holder Variable
Country of Residence	ISO Country Code ±	

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
Monetary Statement	A monetary limit on the value of transactions for which the Certificate can be used. (OID 0.4.0.1862.1.2)	Holder Variable

10.5. 5 Qualified Certificate Profile ±Organisation ±QCP Public

Please note that where a Qualified Organisation Digital Certificate is issued within the meaning of EU Directive 1999/93/EC, the individual applying for the Qualified Organisation Certificate must undergo a face-to-face identity verification procedure.

PURPOSE

The purpose of a Qualified Organisation Digital Certificate is to identify the signatory with a high level of assurance, for the purpose of creating advanced electronic signatures meeting the qualification requirements defined by the applicable legal framework of the Electronic Signatures Directive (1999/93/EC).

These Certificates are issued in accordance Z L W K W K H ³4&3 3XEOLF´ SURILOH GRFXPH issued on a SSCD.

REGISTRATION PROCESS

Validation procedures for QuoVadis Qualified Organisation Digital Certificates are consistent with the Qualified Certificate Policy (QCP public) policy described in ETSI TS101 456.

In all cases, an authorized individual is responsible for all aspects of Certificate management and entering into the QuoVadis Certificate Holder Agreement on behalf of the named organisation.

Evidence of the aut K R U L] H G L Q G L Y L G X D O ¶V Q D P H &Q H &H U W L I L &D W H &K H &N H &G 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 of authorized individual (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.
- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the authorized individual is associated with and authorized by the organisational entity.

FIELDS	CONTENT	DEMARCATION
Subject		
Common Name (CN)	Common Name	Holder Variable
Organisational Unit (OU)	Organisational Unit	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Locality (L)	Locality	

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 Publ		

- Repository ´ PHDQV RQH RU PRUH GDWDEDVHV RI 'LJLWDO &HUWLILFDWHV DQG R Issuing CAs

- Reserved IP Address ´ PHDQV DQ 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 ´ PHDQV 4XR9DGLV &HUWLILFDWH &XUWKH &HUWLILFDWH &XUWKH &HUWLILFDWH being a self-signed Certification Authority that signs Issuing CA Certificates.

- 6HFXUH 6LJQDWXUH &UHDWLRQ '(VLFH ´ 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-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

- Subscriber ´ PHDQV D QDWXUDO RU OHJDO SHUVRQ WKDW KDV HQWHUHG D IRUPDO Digital Certificates to Certificate Holders. The Subscriber may be responsible for the identity vetting of these Certificate Holders. A Subscriber may also hold a Digital Certificate (but is not required to).

- Token ´ PHDQV D &U\SWRJUDSKLF 0RGXOH FRQVLVWLQJ RI D KDUGZDUH REMHFW and microchip.

- Utility Certificate ´ PHDQV D 'LJLWDO &HUWLILFDWH LVVXHG WR D 5HV-Sa RQVLEOH 3H administration of the QuoVadis PKI.

- Validation ´ PHDQV DQ RQOLQH FKHFN E\ 2QOLQH &HUWLILFDWH 6WDWXV 3URWR Certificate Revocation List(s) (in the absence of Online Certificate Status Protocol capability) of the validity of a Digital &HUWLILFDWH DQG WKH YDOLGLW\ RI DQ\ 'LJLWDO &HUWLILFDWH LQ WKDW 'LJ confirming that the Digital Certificate is valid at the time of the check (i.e., it is not revoked or expired).