QuoVadis Root Certification Authority / QuoVadis Root CA1 G3

QuoVadis Root CA3 / QuoVadis Root CA3 G3

Certificate Policy/ Certification Practice Statement

OIDs:	1.3.6.1.4.1.8024.0.1
	1.3.6.1.4.1.8024.0.3
Effective Date:	August 25, 2020
Version:	4.30

Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis

Version Control

Approved by	Date	Version	Comment
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 ElDI-V Revisions
QuoVadis PMA	27 May 2008	4.5	

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

1.2. DOCUMENT NAME, IDENTIFICATION AND APPLICABILITY

The Private Enterprise Object Identifier (OID) assigned by the Internet Assigned Numbers Authority to QuoVadis is 1.3.6.1.4.1.8024. This CP/CPS applies to all CAs and Subscriber Certificates that are signed by the following Root CAs:

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

The inclusion of the TLS/SSL OIDs (1.3.6.1.4.1.8024.0.1.100.1.1 and 1.3.6.1.4.1.8024.0.3.100.1.1) in the certificatePolicies extension of an end entity Subscriber Certificate asserts adherence to and compliance with the Baseline Requirements.

Separate policy documents in the QuoVadis Repository apply to QuoVadis Certificates signed by the following Root CAs:

- Root CA 2 and QuoVadis Root CA 2 G3 (OID 1.3.6.1.4.1.8024.0.2)
- Netherlands PKIoverheid
- QuoVadis Private PKI / Trust Anchor Root CA (OID 1.3.6.1.4.1.8024.0.4)

QuoVadis also operates Time-stamping Authority (TSA) services under a separate QuoVadis Time-Stamp Policy/Practice Statement (OID 1.3.6.1.4.1.8024.0.2000.6). Additional OIDs assigned by QuoVadis include:

HydrantID / Avalanche Cloud Corporation (1.3.6.1.4.1.8024.0.3.900.0)

BEKB - BCBE Issuing CA G2 (1.3.6.1.4.1.8024.0.3.700.0)

HIN Health Info Net CA G2 (1.3.6.1.4.1.8024.0.3.800.0)

1.3. PUBLIC KEY INFRASTRUCTURE PARTICIPANTS

This CP/CPS outlines the roles and responsibilities of all parties involved in the QuoVadis PKI:

- Certification Authorities (CA) (Root and Issuing);
- Registration Authorities (RA);
- Subscribers including Applicants for Certificates prior to issuance; and
- Relying Parties

1.3.1. Certification Authorities

QuoVadis issues Certificates to Subscribers in accordance with this CP/CPS. In its role as a CA, QuoVadis performs functions associated with Public Key operations that include receiving requests; issuing, revoking and renewing a Certificate; and the maintenance, issuance, and publication of CRLs for users within the QuoVadis PKI.

Issuing CAs may be operated by QuoVadis or by other Organisations that have been authorised by QuoVadis to participate within the QuoVadis PKI. Issuing CAs are required to ensure that the services they perform within the QuoVadis PKI are in compliance at all times with their respective Issuing CA Agreements and this CP/CPS.

For Qualified Certificates issued out of the itsme Sign Issuing CA, the Registration Service and Subject Device Provisioning Service are not performed by QuoVadis. These services are performed entirely by Belgian Mobile ID, which undergoes its own audit. In addition, some services are shared

between QuoVadis and Belgian Mobile ID. QuoVadis retains overall responsibility toward relying parties for all Certificates issued from the of the itsme Sign Issuing CA.

In the case of Qualified Certificates, where QuoVadis manages Key Pairs on behalf of the Subscriber, QuoVadis shall ensure:

- where the policy requires the use of a Qualified Electronic Signature/Seal Creation Device (QSCD) then the signatures are only created by the QSCD;
- in the case of natural persons, the Subscribers' Private Key is maintained and used under their sole control and used only for Electronic Signatures; and
- in the case of legal persons, the Subscriber s' Private Key is maintained and used under their control and used only for Electronic Seals.

An Issuing CA may, but shall not be obliged to, detail its specific practices and other requirements in a policy or practices statement adopted by it following approval by the QuoVadis PMA.

Issuing CAs, if authorised to do so by QuoVadis, may rely on third party RAs but retain all responsibility and liability for the fulfilment of Subscriber Identification and Authentication requirements. Issuing CAs are required to conduct regular compliance audits of their RAs to ensure that they are complying their respective RA Agreements and this CP/CPS.

Issuing CAs chaining to a QuoVadis Root must not be used for Man in the Middle (MITM) purposes for the interception of encrypted communications or for traffic management of domain names /IP addresses that the entity does not own or control.

Issuing CAs chaining to a publicly trusted QuoVadis Root must either be technically constrained, or undergo an independent audit and be publicly disclosed in the Repository on the QuoVadis website (https://www.quovadisglobal.com/repository).

1.3.2. Registration Authorities

A Registration Authority (RA) is an entity that performs Identification and Authentication of Certificate Applicants, and initiates or passes along revocation requests foglnd-10.3(tusr)(d Q(s)]TJ/TT3 1 Tf5.2342r.n(T4 1 Tf.9(o8and)

1.3.3. Subscribers

Subscribers are required to act in accordance with this CP/CPS and Subscriber Agreement. A Subscriber

or the Subscriber suspects that it has been compromised. A Subscriber must immediately stop using a Certificate and delete it from the Subscriber's server upon revocation or expiration.

1.3.4. Relying Parties

1.3.5. Other Participants

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable Subscriber Agreement and/or Relying Party Agreement or other relevant QuoVadis documentation. All Application Software Vendors with whom QuoVadis has entered into a contract for inclusion of the QuoVadis Root Certificate as a trusted trust anchor in their software are intended third party participants in the QuoVadis PKI. Accreditation Authorities are granted an unlimited right to re-distribute QuoVadis' Root Certificates and related information in connection with the accreditation.

1.4. CERTIFICATE USAGE

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

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CP/CPS.

1.4.2. Prohibited Certificate Usage

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CP/CPS when the Certificate was issued. Code signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

QuoVadis Certificates shall be used only to the extent the use is consistent with applicable law or regulation, and in particular shall be used only to the extent permitted by applicable export or import laws.

QuoVadis strongly discourages key pinning and does not consider it a sufficient reason to delay revocation. Customers should also take care in not mixing Certificates trusted for the web with non-web PKI. Any Certificates trusted by Application Software Vendors must comply with all requirements of all applicable root distribution policies, incl

Entities submitting Certificate revocation requests must list their identity and explain the reason for requesting revocation. QuoVadis or an RA will authenticate and log each revocation request according to Section 4.9 of this CPS. QuoVadis will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorised representative of the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Affiliated Organisation, QuoVadis or an RA will investigate

3. IDENTIFICATION AND AUTHENTICATION

The Identification and Authentication procedures used by QuoVadis depend on the Class of Certificate being issued (

3.2. INITIAL IDENTITY VALIDATION

QuoVadis may use any legal means of communication or investigation to ascertain the identity of an organisational or individual Applicant in compliance with this CP/CPS. QuoVadis may refuse to issue a

iv) Confirming the Applicant's control over the FQDN through control of an IP address returned from a

i) Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the /.well-known/pki-validation ” directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;

ii) Confirming the Applicant’s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilising the Random Value, performed in accordance with BR Section 3.2.2.5.2;

iii) Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;

iv) Confirming the Applicant’s control over the IP Address by calling the IP Address Contact’s phone number, as identified by the IP Address RA, and obtaining a response confirming the Applicant’s request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;

3.2.6. Criteria For Interoperation

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:

- QuoVadis will perform due diligence on the CA;
- A formal contract must be entered into with QuoVadis, which includes a 'right to audit' clause; and
- The CA must operate under a CPS that meets QuoVadis requirements.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication For Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, QuoVadis creates a new Certificate with the same Certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, QuoVadis may perform some revalidation of the Applicant but may also rely on information previously provided or obtained. QuoVadis does not re-key a Certificate without additional Identification and Authentication if doing so would allow the Subscriber to use the Certificate beyond the limits specified for the applicable Certificate Profile.

3.3.2. Identification and Authentication For Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial Identification and Authentication process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

All revocation requests are authenticated by QuoVadis or the RA responsible for issuing the Certificate. QuoVadis may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised. A Subscriber may request that their Certificate be revoked by:

- Authenticating to a QuoVadis Portal and requesting revocation via that system;
- Applying in person to the RA, Issuing CA or QuoVadis supplying either original proof of identification in the form of a valid Driving License or Passport;
- Telephonic communication using a pre-existing shared secret, password or other information associated with Subscriber's account with the CA following appropriate Identification.

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit A Certificate Application

Either the Applicant or an individual authorised to request Certificates on behalf of the Applicant may submit Certificate Requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to QuoVadis.

QuoVadis does not issue Certificates to entities on a government denied list maintained by the United States or that are located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrolment Process And Responsibilities

Certificate Requests must be in a form prescribed by the Issuing CA and typically include i) an application form including all registration inform

QuoVadis documents potential issuances that were prevented by a CAA record, and may not dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. QuoVadis supports mailto: and https: URL schemes in the iodef record.

The identifying CAA domains recognised by QuoVadis: are digicert.com", digicert. ne.jp", "cybertrust.ne.jp", symantec.com", thawte.com", geotrust.com ", quovadisglobal.com", rapidssl.com", digitalcertvalidation.com" and any domain contain ing those identifying domains as suffixes (e.g. example.digicert.com) or registered country jurisdictions (e.g., digicert.de).

4.3. CERTIFICATE ISSUANCE

4.3.1. CAActions During Certificate Issuance

Certificate issuance is governed by the practices desc

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT HE OR SHE AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT. HE OR SHE ASSUMES A DUTY TO RETAIN CONTROL OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY CONTAINED IN THE CERTIFICATE, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE

QuoVadis may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. QuoVadis may notify Subscribers prior to a Certificate's expiration date. QuoVadis

- Authenticate their identity to the RA.

4.7.4. Notification Of Certificate Re-key To Subscriber

QuoVadis may deliver the Certificate in any secure fashion, such as using a QuoVadis Portal.

4.7.5. Conduct Constituting Acceptance Of A Re-key

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to

as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed; or

xiii) Where the Subscriber becomes unsuitable or unauthorised to hold a Certificate on behalf of an employer or its respective Subsidiaries, Holding Companies or Counterparties.

QuoVadis may revoke any Certificate in its sole discretion, including if QuoVadis believes that:

i) Either the Subscriber or QuoVadis obligations under the CP/CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;

ii) QuoVadis received a lawful and binding order from a government or regulatory body to revoke the Certificate;

iii) The Subscriber is confirmed to be bankrupt, in liquidation, or deceased;

iv) QuoVadis ceased operations and did not arrange for another CA to provide revocation support for the Certificates;

v) The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

vi) The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

vii) For Adobe Signing Certificates, Adobe has requested revocation; or

viii) For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

ix) QuoVadis receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Subscriber that is contained within the Certificate;

x) The Subscriber fails or refuses to comply, or to promptly correct inaccurate, false or misleading

viii) QuoVadis' or the Issuing CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless QuoVadis has made arrangements to continue maintaining the CRL/OCSP Repository;

ix) Revocation is required by the QuoVadis CP/CPS; or

In the case of a PSD2 Certificate, the NCA identified in the Certificate may request revocation by contacting psd2@quovadisglobal.nl. NCA revocation requests are authenticated using either a previously communicated shared secret, or use of a digital signature supported by Qualified Certificate issued to the NCA.

QuoVadis maintains a continuous 24x7 ability to internally respond to high priority revocation requests. Subscribers may also revoke their Certificates via the QuoVadis Portal. For Certificates issued from the itsme sign Issuing CA all revocation requests must be directed to the itsme first-line helpdesk.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. No grace period is permitted once a revocation request has been verified. Issuing CAs will revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time Within Which The CA Must Process The Revocation Request

QuoVadis will revoke a CA Certificate within one hour after receiving clear instructions from the PMA.

Within 24 hours after receiving a Certificate problem report, QuoVadis investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

For Certificates containing the ETSI OIDs defined in section 10.1.1 the maximum delay between the receipt of the revocation request and the update of the Certificate status information is at most 24 hours. For Certificates issued from the itsme sign Issuing CA, this 24 hour time period starts with the receipt of the revocation request at the itsme first-line helpdesk.

4.9.6. Revocation Checking Requirement For Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the Certificate path in accordance with IETF PKIX standards, including checking for Certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7. CRL Issuance Frequency

QuoVadis uses its offline Root CAs to publish CRLs for its Issuing CAs at least every 6 months and within 18 hours after revoking an Issuing CA Certificate. QuoVadis updates the CRL for end-user Certificates at least every 12 hours and the date of the Next Update" field will not be more than 3 calendar days after the date in the field Effective Date". A CRL is valid for a maximum of 72 hours.

Before revoking an Issuing CA Certificate a last CRL is generated with a nextUpdate field value of "99991231235959Z". QuoVadis doesnot issue a last CRL until all Certificates in the scope of the CRL are

Upon expiry of the Issuing CA, the associated OCSP Re

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The section of the CP/CPS provides a high level description of the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by QuoVadis to provide trustworthy and reliable CA operations. QuoVadis maintains a security program to:

i) Protect the confidentiality, integrity, and availability of data and business process;

ii) Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of data and business process;

iii) Protect against unauthorised or unlawful access, use, disclosure, alteration, or destruction of data and business process;

iv) Protect against accidental loss or destruction of, or damage to data and business processes; and

v) Comply with all other security requirements applicable to the CA by law and industry best practices.

QuoVadis performs an annual risk assessment to identify internal and external threats and assess likelihood and potential impact of these threats to data and business processes.

5.1. PHYSICAL CONTROLS

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

5.1.1. Site Location and Construction

QuoVadis performs its CA and TSA operations from secure datacentres located in Bermuda, the Netherlands, and Switzerland. The data centres are equipped with logical and physical controls that make QuoVadis' CA and TSA operations inaccessible to non-trusted personnel. QuoVadis operates under a security policy designed to detect, deter, and prevent unauthorised access to QuoVadis' operations.

5.1.2. Physical Access

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

5.1.3. Power And Air Conditioning

Datacentres have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and generators provide redundant backup power.

5.1.4. Water Exposures

The cabinets housing QuoVadis' CA and TSA systems are designed to prevent and protect against water exposure.

5.1.5. Fire Prevention And Protection

QuoVadis datacentres are equipped with fire suppression mechanisms.

5.1.6. Media Storage

5.2.1.5. RA Administrators

RA Administrators manage the RA certificate management systems.

5.2.1.6. Security Officers

The Security Officer is responsible for administering and implementing security practices.

5.2.2. Number of Persons Required per Task

QuoVadis requires that at least two people acting in a trusted role take action for the most sensitive tasks,

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met by QuoVadis due to a prohibition or limitation

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types Of Events Recorded

QuoVadis records details of the actions taken to process a Certificate Request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate Request.

QuoVadis logs the following events:

- CA key lifecycle management events;
- CA and Subscriber Certificate lifecycle management events;
- Security events, including
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

QuoVadis event logs include:

- Date and time of the entry
- Serial or sequence number of entry (for automatic journal entries)
- Details of the of entry (name, type, etc.)
- Source of entry (for example, terminal, port, location, customer, IP address)
- Destination address (if relevant)
- Identity of the entity making the journal entry (e.g. User ID)

5.4.2. Frequency Of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3. Retention Period For Audit Log

QuoVadis audit logs are retained for at least seven years. Audit logs relating to the Certificate lifecycle are retained as archive records for a period no less than eleven (11) years for Swiss Qualified Certificates and for seven (7) years for all other Certificates starting from the expiration of the Certificate. Certain high volume system generated logs are retained for 18 months based on a risk assessment.

5.4.4. Protection Of Audit Log

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/or Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures

Each Issuing CA performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing CA's premises and storage at a secure, off-site location.

required by law. QuoVadis maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If QuoVadis needs to transfer any media to a different archive site or equipment, QuoVadis will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements For Time Stamping Of Records

QuoVadis 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.

5.5.6. Archive Collection System

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

5.5.7. Procedures To Obtain And Verify Archive Information

Only specific QuoVadis Trusted Roles and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their authorised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

5.6. KEY CHANGEOVER

Key changeover is not automatic, but procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, QuoVadis ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs and OCSP responder Certificates associated with that key. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

QuoVadis maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. QuoVadis reviews, tests, and updates its incident response plans and procedures on a periodic basis.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

QuoVadis makes regular system backups weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If Qu

5.7.3. Entity Private Key Compromise Procedures

If QuoVadis suspects that one of its CA Private Keys has been compromised, the PMA will convene a response team to assess the incident and take appropriate action. Specifically, QuoVadis will:

i) Collect information related to the incident;

ii) Determine the degree and scope of compromise; and report on the course of action that should be taken to correct the problem and prevent reoccurrence;

iii) If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures; and

iv) Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

QuoVadis may generate a new Key Pair and sign a new Certificate. If a disaster physically damages QuoVadis' equipment and destroys all copies of QuoVadis' Private Keys then QuoVadis will provide notice to affected parties at the earliest feasible time.

5.7.4. Business Continuity Capabilities After a Disaster

To maintain the integrity of its services, QuoVadis implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving QuoVadis' primary facility and that QuoVadis be capable of maintaining other services or resuming them as quickly as possible following a disaster. QuoVadis periodically reviews, tests, and updates the BCMP and supporting procedures.

5.8. CA AND/OR RA TERMINATION

Before terminating its CA or RA activities, QuoVadis will:

i) Notify relevant Government and Certification bodies under applicable laws and related regulations;

ii) Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors and by posting such information on QuoVadis' web site; and

iii) Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, QuoVadis will:

i) transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;

ii) revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;

iii) destroy all Private Keys; and

iv) make other necessary arrangements that are in accordance with this CP/CPS.

For Qualified Certificates, 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 EU Qualified Certificates, 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.

QuoVadis has made arrangements to cover the costs associated with fulfilling these requirements in case

6.1.4. CAPublic Key To Relying Parties

QuoVadis' Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root stores, and/or as roots signed by other CAs. All accreditation authorities supporting QuoVadis Certificates and all application software providers are permitted to redistribute QuoVadis root anchors.

QuoVadis may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may also obtain QuoVadis CA Certificates from QuoVadis' web site or by email.

6.1.5. Key Sizes

QuoVadis follows the relevant ETSI and NIST guidance in using and retiring signature algorithms and key sizes. Key sizes for individual Certificate Profiles are disclosed in Appendix A and Appendix B. Currently QuoVadis generates and uses at least the following key sizes, signature algorithms and hash algorithms for signing Certificates, CRLs and OCSP responses:

- 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8);
- 256-bit ECDSA Key or greater with the matching Secure Hash Algorithm version as required; or
- a hash algorithm that is equally or more resistant to a collision attack allowed by the references in sections 1.1 and 8.1.

QuoVadis requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms. QuoVadis may require higher bit keys in its sole discretion.

Any Root Certificates participating in the AATL program issued after July 1, 2017 must be at least 3072-bit for RSA and 256-bit for ECDSA.

QuoVadis and Subscribers may fulfill transmission security requirements using TLS/SSL or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

6.1.6. Public Key Parameters Generation And Quality Checking

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

All Participants in the QuoVadis PKI are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this QuoVadis CP/CPS. Without limitation to the generality of the foregoing, all Participants in the QuoVadis PKI must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised

6.2.6. Private Key Transfer Into Or From A Cryptographic Module

All CA keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, QuoVadis encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access. If QuoVadis becomes aware that an Issuing CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Issuing CA, then QuoVadis will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If QuoVadis pre-generates Private Keys and transfers them into a hardware token, for example transferring generated end-entity Subscriber Private Keys into a smart card, it will securely transfer such Private Keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Keys.

6.2.7. Private Key Storage On Cryptographic Module

CA Private Keys are generated and stored in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. Root CA Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

6.2.8. Method Of Activating Private Key

QuoVadis' Private Keys are activated according to the specifications of the HSM manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate Profile. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers. When deactivated, Private Keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys.

6.2.9. Method Of Deactivating Private Key

QuoVadis' Private Keys are deactivated via manual and passive logout procedures on the applicable HSM device when not in use. QuoVadis never leaves its HSM devices in an active unlocked or unattended state.

For Qualified Certificates, the Subscriber Private Keys are generated and stored on a QSCD.

For relevant Qualified Certificates, in accordance with the eIDAS Regulation, the Subscriber Private Keys are generated and stored on a QSCD that meets the requirements laid down in Annex II of eIDAS and is certified to the appropriate standards. Where QuoVadis manages the QSCD on behalf of the Subscriber, QuoVadis operates the QSCD in accordance with Annex II of eIDAS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

Public Keys will be recorded in Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained.

6.3.2. Certificate Operational Periods And Key Pair UsagePeriods

Please see the variable Issuing CA 'Valid From' and 'Valid To' fields in the Certificate Profiles outlined in Appendix A. The maximum validity periods for Certificates issued within the QuoVadis PKI are:

Type	Certificate Term
Publicly Trusted Root CAs	30 years
Publicly Trusted Issuing CAs	10 - 15 years
Qualified Certificates	1 to 3 years
TLS/SSL Certificates	825 days (397 days starting September 1, 2020)
All other Certificates	1 to 3 years

Participants shall cease all use of their Key Pairs after their usage periods have expired. Relying Parties may still validate signatures generated with these keys after expiration of the Certificate.

QuoVadis may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. QuoVadis does not issue Subscriber Certificates with an expiration date that exceeds the Issuing CA's term or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation And Installation

QuoVadis activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer, meeting the requirements of FIPS 140-2 Level-3 and/or Common Criteria EAL 4. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CP/CPS. QuoVadis will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delive

must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Subscriber's personal information.

6.4.3. Other Aspects Of Activation Data

Where a PIN is used, the User is required to enter the PIN and identification details such as their Distinguished Name before they are able to access and install their Keys and Certificates.

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 QuoVadis PMA and is communicated to all employees.

6.5.1. Specific Computer Security Technical Requirements

QuoVadis secures its CA systems and authenticates and protects communications between its systems and trusted roles. QuoVadis' CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

RAs must ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

QuoVadis' CA systems are configured to:

i) authenticate the identity of users before permitting access to the system or applications;
ii) manage the privileges of users and limit users to their assigned roles;
iii) generate and archive audit records for all transactions;
iv) enforce domain integrity boundaries for security critical processes; and
v) support recovery from key or system failure.

All Certificate Status Servers:

i) authenticate the identity of users before permitting access to the system or applications;
ii) manage privileges to limit users to their assigned roles;
iii) enforce domain integrity boundaries for security critical processes; and
iv) support recovery from key or system failure.

QuoVadis enforces multi-factor authentication on any Portal account capable of directly causing Certificate issuance.

6.5.2. Computer Security Rating

A version of the core CA software used by QuoVadis has obtained the Common Criteria EAL 4+ certification.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

QuoVadis has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. QuoVadis only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision

of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by QuoVadis are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to QuoVadis' operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

QuoVadis has mechanisms in place to control and continuously monitor the security-related configurations of its CA systems. When loading software onto a CA system, QuoVadis verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

QuoVadis CA and RA functions are performed using networks secured in accordance to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

QuoVadis documents and controls the configuration of its systems, including any upgrades or modifications made. Root Keys are kept offline and brought online only when necessary to sign Issuing CA Certificates, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

The QuoVadis security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled.

6.8. TIME-STAMPING

The QuoVadis Time-stamping Authority (TSA) 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 TSA such that Participants and Relying Parties may evaluate their confidence in the operation of the time- stamping services.

The QuoVadis Time-Stamp Policy/Practice Statement is structured in accordance with ETSI EN 319 421 and should be read in conjunction with this CP/CPS. The QuoVadis Time-stamp Policy aims to deliver time-stamping services used in support of either Swiss or eIDAS Qualified Electronic Signatures, as well as any application requiring proof that a datum existed before a particular time.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFIILE

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

7.1.1. Basic Certificate Contents

Fields	Content	Demarcation
Version	QuoVadis certificates are Version 3	Fixed
Serial Number	Unique system generated random number assigned to each certificate, containing at least 64 bits of output.	Fixed
Signature Algorithm	The algorithm identifier for the algorithm used to sign the certificate.	Fixed
Issuer	Issuer is the entity that has signed and issued the certificate	
Common Name (CN)	Issuing CA Common Name	Fixed
Organisational Unit (OU)	Issuing CA	Fixed

7.1.2. Certificate Extensions

The extensions defined for X.509 v3 Certificates provide methods for associating additional attributes with users or Public Keys and for managing relationships between CAs.

The table below describes common Certificate extensions that are included in QuoVadis Certificates. Refer to Appendix A and Appendix B for Certificate extensions that are specific to the individual Certificates Classes.

Fields	Content	Demarcation
Extensions		
Authority Key Identifier		

Fields	Content	Demarcation
	http://crl.quovadisglobal.com/<caname>.crl (where <caname> is the short name of the relevant CA)	
Authority Information Access	Indicates how to access information and services for the issuer of the Certificate. The following URLs are included in QuoVadis Certificates: URL = http://ocsp.quovadisglobal.com URL=http://trust.quovadisglobal.com/<caname>.crt (where <caname> is the short name of the relevant CA)	Fixed
Basic Constraints	Indicates whether the subject of the Certificate is a CA and the maximum depth of valid certification paths that include this Certificate.	Fixed
Thumbprint Algorithm	The algorithm used to hash the Certificate	Fixed
Thumbprint	The system generated hash of the Certificate	Fixed

7.1.3. Algorithm Object Identifiers

QuoVadis Certificates are signed using one of the following algorithms:

sha256WithRSAEncryption[9]	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha256[10]	[iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2]
ecdsa-with-SHA384[11]	[iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3]

QuoVadis and Subscribers may generate Key Pairs using the following:

id-dsa	[iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1]
RsaEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1]
Dhpublicnumber	[iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1]
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
id-ecPublicKey	[iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1]

Elliptic curve Public Keys submitted to QuoVadis for inclusion in end entity Certificates should be based on NIST Suite B" curves.

7.1.4. Name Forms

See Appendix A and Appendix B.

Each Certificate includes a serial number that is unique to the Issuing CA. Optional subfields in the subject of an TLS/SSL Certificate must either contain information verified by QuoVadis or be left empty.L Cert4atrTJEf6.7jo3r.9.8(e)-1. rn

7.1.5.1. Name-Constrained serverAuth CAs

If the technically constrained Issuing CA Certificate incl

7.2. CRL PROFILE

7.2.1. Version Number

QuoVadis issues X.509 version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	QuoVadis Issuing CA name
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date

7.5.2. QuoVadis Root Certificate Hashes

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

7.5.2.1. QuoVadis Root CA Certificate Hashes

Field	Certificate Profile
Serial Number	3ab6508b
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash (sha1): 86 26 cb 1b c5 54 b3 9f bd 6b ed 63 7f b9 89 a9 80 f1 f4 8a 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 1 G3 Certificate Hashes

Field	Certificate Profile
Serial Number	58 [illegible]

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY, CIRCUMSTANCE AND STANDARDS OF ASSESSMENT

CAs and RAs following this CP/CPS are subject to Internal Audit as well as annual audits by an independent external auditor to assess compliance where applicable to the following standards and requirements:

Standards / Law	
WebTrust	WebTrust Principles and Criteria for Certification Authorities WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
SR 943.03 [ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016
SR 943.032 [VZertES]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016
SR 943.032.1 [TAV]	R 943.032.1 / Anhang: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate Ausgabe 1: 23.11.2016 Inkrafttreten: 1.1.2017
ESI (Directive")	Electronic Signatures and Infrastructures (ESI) regulations from EU

Publicly available audit reports provided by Conformance Assessment Bodies responsible for these audits will be published at https://www.quovadisglobal.com/accreditations. Compliance audits as carried out under these provisions may substitute for audits noted in this CP/CPS.

8.2. IDENTITY AND QUALIFICATIONS OF ASSESSOR

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements. ETSI Conformance Assessment Bodies must meet the requirements of the relevant national accrediting authority. Auditors shall be experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies.

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

Audits as applicable cover QuoVadis' business practices disclosure, the integrity of QuoVadis' PKI operations, and an Issuing CAs' compliance with this CP/CPS and referenced requirements. Audits verify that QuoVadis is compliant with the CP/CPS and applicable standards and regulatory requirements.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to QuoVadis' services, then (i) the auditor will document the discrepancy, (ii) the auditor will promptly notify QuoVadis, and (iii) QuoVadis will develop a plan to cure the noncompliance. QuoVadis will submit the plan to the PMA for approval and to any third party that QuoVadis is legally obligated to satisfy. The PMA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. QuoVadis is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the PMA to address the non-compliant Issuing CA.

For Qualified Certificates the course of action and time frame for rectification of any deficiency as set by the relevant accrediting authority must be followed.

8.6. COMMUNICATION

9.2.4. Fiduciary Relationships

QuoVadis is not the agent, fiduciary or other representative of any Subscriber and/or Relying Party and must not be represented by the Subscriber and/or Relying Party to be so. Subscribers 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 Subscriber 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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

QuoVadis follows the Privacy Notices posted on its website when handling personal information. See https://www.quovadisglobal.com/privacy-policy. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9.4.2. Information Treated As Private

QuoVadis treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. QuoVadis protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Deemed Not Private

Subject to local laws, private information does not include CP/CPS and other Repository documents, Certificates, CRLs, or their contents.

9.4.4. Responsibility To Protect Private Information

QuoVadis employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. QuoVadis will not divulge any private Subscriber information to any third party for any reason, unless compelled to do so by law or competent regulatory authority. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice And Consent To Use Private Information

In the course of accepting a Certificate, individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the QuoVadis CA, and used as explained in the registration process. They have also been given an oppot5.9(doI)t All I823 Tw12 90 (05 -s)5.9(I)823 Tw12 90 (05 -s)5.9(d9(t a

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

QuoVadis makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

9.6.2. RA Representations And Warranties

RAs represent and warrant that:

i) The RA's certificate issuance and management services conform to the QuoVadis CP/CPS and applicable CA or RA Agreements;

ii) Information provided by the RA does not contain any false or misleading information;

iii) Reasonable steps are taken to verify that the information contained in any Certificate is accurate at the time of issue;

iv) Translations performed by the RA are an accurate translation of the original information;

v) All Certificates requested by the RA meet the requirements of this CP/CPS and RA Agreement; and

vi) The RA will request that Certificates be revoked by QuoVadis if they believe or are notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

QuoVadis' RA Agreement may contain additional representations. Subscriber Agreements may include additional representations and warranties.

9.6.3. Subscriber Representations And Warranties

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any

PARTICULAR PURPOSE, AND NON-INFRINGEMENT. QUOVADIS DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE. QuoVadis does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time. Subscriber's sole remedy for a defect in the Certificates is for QuoVadis to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that QuoVadis has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Certificates or combination of the Certificates with other products and services by parties other than QuoVadis, or (ii) Subscriber's breach of any provision of the Subscriber Agreement.

9.8. LIABILITY AND LIMITATIONS OF LIABILITY

This Section 9.8 does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CP/CPS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) QUOVADIS AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNE

reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorised use of a Certificate or Private Key caused by the Subscriber's negligence or intentional

and without changing the version number. The QuoVadis PMA is responsible for determining what constitutes a material change of the CP/CPS.

9.12.3. Circumstances Under Which Object Identifiers Must Be Changed

The QuoVadis PMA is solely responsible for determining whether an amendment to the CP/CPS requires an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

To the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Participant shall notify QuoVadis, and any other party to the dispute for the purpose of seeking business resolution. Both Participant and QuoVadis shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this CP/CPS and other relevant agreements.

i) Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.

ii) Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that

10. APPENDIXA

10.1. CERTIFICATE

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	Relevant to the Policy in ETSI EN 319 411-2 for:			
	EU Qualified Certificates issued to a natural person (QCP-n-qscd), with the OID 0.4.0.194112.1.2	ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd)		
	EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the OID 0.4.0.194112.1.3	0.4.0.194112.1.3 (QCP-l-qscd)		

10.1.2. Key Usage And Escrow

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

Certificate Type	Key Usage/ Extended Key Usage Options	Applicability 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 documentSigning	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow only permitted for certain Issuing CAs. Not permitted for any CAs on EUTL)	Allowed (Escrow not permitted)	Not Allowed
Signing	Key Usage digitalSignature nonrepudiation Extended Key Usage smartcardlogon clientAuth emailProtection documentSigning	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)
Encryption	Key Usage keyEncipherment Extended Key Usage emailProtection	Allowed (Escrow permitted)	Allowed (Escrow permitted)	Allowed (Escrow not permitted)	Not Allowed
Authentication	Key Usage digitalSignature Extended Key Usage smartcardlogon clientAuth	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Allowed (Escrow not permitted)	Not Allowed

The Certificate Profiles that follow indicate the fields which are VARIABLE on initial registration by the Subscriber (Holder Variable") and those which are FIXED by the Issuing CA either based on policy or by IETF Standard, applicable law, or regulation.

10.2. QV STANDARD

Purpose
Standard Certificates provide flexibility for a range of us

If the subject is a natural person evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national

Extended Key Usage	clientAuth emailProtection documentSigning	Variable

10.4. QV ADVANCED +

Purpose
QuoVadis Advanced+ Certificates are used for the same purposes as QuoVadis Advanced Certificates, with the only difference being that they are issued on a Secure Cryptographic Device. The QuoVadis Advanced+ Certificate Class is trusted in the Adobe Approved Trust List (AATL). Swiss Regulated Certificates issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ Certificate Class.
Registration Process
QuoVadis Advanced+ Certificates are based on with the Normalised Certificate Policy (NCP+) described in ETSI EN 319 411-1. Unless the Subscriber 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 Subscriber shall include the following: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. If the subject is a natural person 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 subject is a natural person who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. If the Subscriber is a natural person who is identified in association with a legal person (organisational entity), additional evidence shall be provided of: • Full name and legal status of the associated legal person; • Any relevant existing registration information (e.g. company registration) of the associated legal person; and • Evidence that the Subscriber is affiliated with the legal person. If the Subscriber is a legal person (organisational entity), evidence shall be provided of: • Full name of the legal person; and • Reference to a nationally recognized registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name. If the Subscriber is a device or system operated by or on behalf of a legal person, evidence shall be provided of: • identifier of the device by which it may be referenced (e.g. Internet domain name);

- full name of the organisational entity;
- a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

QuoVadis Advanced+ Certificates must be issued on a Secure Cryptographic Device and adhere to the following requirements:

- Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA or RA;
- User activation data is securely prepared and distributed separately from the Secure Cryptographic Device;
- If keys are generated under the Subscriber's control, they are generated within the Secure Cryptographic Device used for signing or decrypting;
- The Subscriber's Private Key can be maintained under the subject's sole control; and
- Only use the Subscriber's Private Key for signing or decrypting with the Secure Cryptographic Device.

Attribute	Values	Comment
Subject	/CN (mandatory)	

10.4.1. Swiss Regulated Certificate issued to a Natural Person

Purpose

	/E (optional) /L (optional) /ST (optional) /C (mandatory)	
SAN	/E 1.3.6.1.4.1.311.20.2.3 UPN	Variable
Certificate Policies	1.3.6.1.4.1.8024.1.300 QV Advanced+ Certificate 0.4.0.2042.1.2 ETSI NCP+ OID URL: https://www.quovadisglobal.com/repository User Notice: Regulated certificate	Fixed
Adobe Acrobat Trust List	1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA) 1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	Optional
Key Usage	digtalSignature	Fixed/Critical
Extended Key Usage	clientAuth emailProtection smartcardlogon	Fixed

10.4.2. Swiss Regulated Certificate issued to a Legal Person (Company Seal)

Purpose
Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QV Advanced+ Certificate Class. Swiss Regulated Certificates are issued out of the QuoVadis Swiss Regulated CAs" and have the notice text regulated certificate" in the CertificatePolicies user notice.
Registration Process

Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVadis Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates.

For the issuance and life cycle management of Swiss Regulated Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant Qualified Certificate.

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence by an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence

- 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.

Evidence of the Certificate applicant 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 according to ZertES. 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

eIDAS Regulation. These Certificates meet the relevant ETSI Policy for EU Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd).

	/T (optional) /O (optional) /OU (optional) /serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory) If serialNumber is present then it must be structured per section 5.1.3 of ETSI EN 319 412-1: • 3 character identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier.	
SAN	/E	Optional
Certificate Policies	1.3.6.1.4.1.8024.1.400 QV Qualified QSCD, or 1.3.6.1.4.1.8024.1.410 QV Qualified QSCD -on behalf of 0.4.0.194112.1.2 (QCP-n-qscd) URL: https://www.quovadisglobal.com/repository User Notice: Qualified certificate	Fixed Only Swiss Qualified
Adobe Acrobat Trust List	1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA) 1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	Optional
Key Usage	Nonrepudiation digitalSignature keyEncipherment (optional)	Fixed/Critical
Extended Key Usage	clientAuth emailProtection documentSigning	Fixed
qcStatements		
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-4	esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD.	Fixed
id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6	esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014	Fixed

id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	URL=
id-etsi-qcs-5	https://www.quovadisglobal.com/repository

	/GN (mandatory if CN without Pseudonym) /SN (mandatory if CN without Pseudonym) Pseudonym (optional) /T (optional) /O (optional) /OU (optional) /serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory) If serialNumber is present then it must be structured per section 5.1.3 of ETSI EN 319 412-1: • 3 character identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier.	Variable
SAN	/E	Optional
Certificate Policies	1.3.6.1.4.1.8024.1.450 QV Qualified no QSCD, or 1.3.6.1.4.1.8024.1.460 QV Qualified no QSCD – on behalf of 0.4.0.194112.1.0 (QCP-n) URL: https://www.quovadisglobal.com/repository	Fixed
Key Usage	digitalSignature nonRepudiation	Fixed/Critical
Extended Key Usage	emailProtection documentSigning	Fixed
qcStatements		
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6	esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 1 = Certificate for electronic Signatures as defined in Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5 id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	URL= https://www.quovadisglobal.com/repository Language = EN	Fixed

id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed

10.5.3. eIDAS Qualified Certificate issued to a Legal Person on a QSCD

Purpose
The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation. This type of QuoVadis Qualified Certificates uses a QSCD for the protection of the private key. These Certificates meet the relevant ETSI Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd). QuoVadis recommends that QCP-l-qscd certificates are used only for electronic seals. The content of these Certificates meet the relevant requirements of: • ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures • ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons • ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements • ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
Registration Process
Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for Policy for EU qualified certificate is sued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd). The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified: • by the physical presence by an authorised representative of the legal person; or • using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N°910/2014 [i.1]. Evidence shall be provided of: • Full name of the organisational entity consistent with the national or other applicable identification practices); and • When applicable, the association between the legal person and the other organisational entity

national public register, EBA PSD2 Register, EBA Credit Institution Register or authenticated letter). QuoVadis also confirms the PSD2 role(s) of the Certificate Applicant (RolesOfPSP) in accordance with the rules for validation provided by the NCA, if applicable:

- i) account servicing (PSP_AS)
  OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
- ii) payment initiation (PSP_PI)
  OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
- iii) account information (PSP_AI)
  OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
- iv) issuing of card-based payment instruments (PSP_IC)
  OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }

These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

Attribute	Values	Comment
Subject	/CN (mandatory) =/0 /O (optional) /OU (optional) /serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory) If serialNumber is present then it must be structured per section 5.1.3 of ETSI EN 319 412-1: • 3 character identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier. For PSD2: • PSD" as 3 character legal person identity type reference; • 2 character ISO 3166 [7] country code representing the NCA country; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • 2-8 character NCA identifier (A-Z uppercase only, no separator) • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • PSP identifier (authorisation number as specified by the NCA).	See definitions in section 7.1.1 Variable
SAN	/E	Optional

Certificate Policies	1.3.6.1.4.1.8024.1.400 or 1.3.6.1.4.1.8024.1.410 or QV Qualified -QSCD 0.4.0.194112.1.3 (QCP-l-qscd) URL: https://www.quovadisglobal.com/repository	Fixed
Adobe Acrobat Trust List	1.2.840.113583.1.1.9.1 Adobe Time-stamp (link to TSA) 1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	Optional
Key Usage	Nonrepudiation digitalSignature (optional)	Fixed/Critical
Extended Key Usage	documentSigning (optional) emailProtection clientAuth (optional)	Fixed
qcStatements		
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-4	esi4-qcStatement-4: The private key related to the certified public key resides on a QSCD.	Fixed
id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6	esi4-qcStatement-6 : Type of certificate id-etsi-qcs-QcType 2 = Certificate for electronic Seals as defined in Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5	URL= https://www.quovadisglobal.com/repository Language = EN	Fixed
id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is included in QuoVadis Certificates	Fixed
id-etsi-psd2-qcStatement (0.4.0.19495.2)	PSD2QcType ::= SEQUENCE{rolesOfPSP RolesOfPSP, nCAName NCAName,nCAId NCAId}	Only for PSD2 Variable Refer to: ETSI TS 119 495 5.1

•

	/serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory) If serialNumber is present then it must be structured per section 5.1.3 of ETSI EN 319 412-1: • 3 character identity type reference (e.g. PAS or IDC); • 2 character ISO 3166 country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier. For PSD2: • PSD" as 3 character legal person identity type reference; • 2 character ISO 3166 [7] country code representing the NCA country; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • 2-8 character NCA identifier (A-Z uppercase only, no separator) • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • PSP identifier (authorisation number as specified by the NCA).	
SAN	/E	Variable
Certificate Policies	1.3.6.1.4.1.8024.1.450 QV Qualified –no QSCD 0.4.0.194112.1.1 (QCP-l) URL: https://www.quovadisglobal.com/repository	Fixed
Key Usage	digitalSignature nonRepudiation	Fixed/Critical
Extended Key Usage	documentSigning emailProtection	Fixed
qcStatements		
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed
id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-6	esi4-qcStatement-6: Type of certificate id-etsi-qcs-QcType 2 = Certificate for electronic Seals as defined in Regulation EU No 910/2014	Fixed

id-etsi-qcs-QcPDS (0.4.0.1862.1.5) id-etsi-qcs-5	URL= https://www.quovadisglobal.com/repository Language = EN	Fixed
id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	0.4.0.194121.1.2 optional semantics identifier OID (id-etsi-qcs- SemanticsId-Legal) that is indeW(E)7.7(N)5ed in QA Tc0 Tw( )34r cJT*-Cert 1.12(ific5(c)ht)TJ2es8 Tc0 Tw[(Fix	

QV Qualified Switzerland Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour.		
Attribute	Values	Comment
Subject	/CN (mandatory) = Natural Person (/GN+/SN or Pseudonym) /GN (mandatory if CN without Pseudonym)	

10.7. QV CLOSED COMMUNITY

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

Certificates issued by Closed Community Issuing CAs are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone CP/CPS to its community issue various Certificates in accordance with the CP/CPS.

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

Under no circumstances ca

10.7.1.1. Grid End User Certificate

Purpose

10.7.1.2. 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 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 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.		
Attribute	Values	Comment
Issuer	QuoVadis Grid ICA / QuoVadis Grid ICA G2 QuoVadis Limited BM	Fixed
Validity	Maximum Certificate lifetime of 1 year	Fixed
Subject	/CN /O (mandatory) /OU (optional) /L (optional) /ST (optional) /C (mandatory)	See definitions in section 7.1.1 Variable
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=<organisation identifier>, DC=hosts	Holder Variable
SAN	SAN dNSName with the Fully Qualified Domain Name or an iPAddress	Variable
Certificate Policies	1.3.6.1.4.1.8024.0.1.10.0.0 QV Grid ICA 1.2.840.113612.5.2.2.1 IGTF Classic Authentication Profile	Fixed
Key Usage	digitalSignature keyEncipherment dataEncipherment	Fixed/Critical
Extended Key Usage	clientAuth serverAuth	Fixed

11. APPENDIXB

11.1. BUSINESS SSL

Field	Value
Validity Period	1 or 2 years expressed in UTC format. Effective September 1, 2020: maximum 397 days.
Subject Distinguished Name	
Organisation Name	subject:organisationName (2.5.4.10)
Organisation Unit	subject:organisationUnit (2.5.6.5)

QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended 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
- That it is safe" to do business with the Subject named in the Certificate.

Eligible Applicants

Individuals (natural persons), incorporated entities, government entities, general partnerships, unincorporated associations, and sole proprietorships may apply for QuoVadis Business SSL Certificates.

Verification Requirements

Identity: QuoVadis verifies the identity and address of the organisation and that the address is the Applicant's address of existence or operation. QuoVadis verifies the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

i) A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

ii) A third party database that is periodically updated and considered a Reliable Data Source;

iii) A site visit by the CA or a third party who is acting as an agent for the CA; or

iv) An Attestation Letter.

DBA/Tradename: If the Subject Identity Information is to include a DBA or tradename, QuoVadis verifies the Applicant's right to use the DBA/tradename using at least one of the following:

i) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

ii) A Reliable Data Source;

iii) Communication with a government agency responsible for the management of such DBAs or tradenames;

iv) An Attestation Letter accompanied by documentary support; or

v) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identifistoc.t the CA determines to be reliable.

Verification of Country: QuoVadis verifies the country associated with the Subject using one of the following:

i) the IP Address range assignment by country for either (i) the web site's IP

ii) address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;

iii) the ccTLD of the requested Domain Name;

iv) information provided by the Domain Name Registrar; or

v) a method identified in Identity" above.

Application Process

During the Certificate approval process, QuoVadis Validation Specialists employ controls to validate the identity of the Applicant and other information featured in the Certificate Application to ensure compliance

Step 2: QuoVadis independently verifies information using a variety of sources.

Step 3: The Applicant accepts the Subscriber Agreement and approves Certificate issuance. Step 4: All signatures are verified through follow-up procedures or telephone calls.

Step 5: QuoVadis obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the Certificate Request and notify the Applicant accordingly. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 6: QuoVadis creates the Business SSL Certificate.

Step 7: The Business SSL Certificate is delivered to the Applicant.

Renewal

Renewal requirements and procedures include verification that the Applicant continues to have authority to use the domain name, and that the Certificate Application is approved by an authorised representative of the Applicant.

11.2. CODE SIGNING

Field	Value	Comments
Validity Period	1, 2, or 3 years expressed in UTC format	
Subject Distinguished Name		
Organisation Name	subject:organisationName (2.5.4.10)	Required field. The Subject's verified legal name.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Optional field. Must not include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless QuoVadis has verified this information
Common Name	subject:commonName (2.5.4.3)	Required field. The Subject's verified legal name.
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)	Required if the subject:localityName field is absent. Optional if the subject:localityName fields is present.
Locality	subject:locality (2.5.4.6)	Required if the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field is present.
Country	subject:countryName (2.5.4.6)	Required field.
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)	

Extension	Value	
Authority Key Identifier	c=no; Octet String	
Subject Key Identifier	c=no; Octet String	
Key Usage	c=yes; Digital Signature (80)	
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codesSigning)	
Field	Value	Comments
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; { 2.23.140.1.4.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository	1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID. 2.23.140.1.2.3 is the Code Signing Minimum Requirements OID.
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =http://ocsp.quovadisglobal.com - id-ad-caIssuers (CA Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/<CA Name>.crt	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/<CA Name>.crl	

Purposes of Code Signing

The primary purpose of QuoVadis Code Signing Certificates is to establish that executable code originates from a source identified by QuoVadis. QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended 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
- That it is safe" to do business with the Subject named in the Certificate.

Eligible Applicants

Eligible Applicants include Individual Applicants and Organisational Applicants.

An Individual Applicant is an Applicant that is an individual and requests a Certificate that will list the Applicant's legal name as the Certificate subject.

An Organisational Applicant is an Applicant that requests a Certificate subject other than the name of an individual. Organisational Applicants include priv

Application Process

During the Certificate approval process, QuoVadis Validation Specialists employ controls to validate the

12. APPENDIXC

12.1. DEFINITIONS AND ACRONYMS

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

Advanced Electronic Signature means an Electronic Signature which meets the requirements set out in Article 26 of the eIDAS Regulation.

Applicant means an entity applying for a Certificate.

Application Software Vendors means a software developer whose software displays or uses QuoVadis Certificates and distributes QuoVadis' Root Certificates.

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

Authority Letter is a signed by a Confirming Person acting for the Applicant for EV Certificates to establish the authority of individuals to act as the Subscriber's agents.

Authorisation Number : A unique identifier of a Payment Service Provider acting as the Subscriber for PSD2 Certificates. The Authorisation Number is used and recognised by the NCA.

Authorisation Domain Name: The Domain Name used to obtain authorisation for certificate issuance for a given FQDN as defined by the Baseline Requirements.

Authentication means the procedures and requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to provide against fraud, imitation and deception (Authenticate" and Authenticated" to be construed accordingly).

Certificate Approver is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorise other employees or third parties to act as a Certificate Requesters, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certificate Application Any of several forms completed by Applicant or QuoVadis and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

Certification means the process of creating a Certificate for an entity and binding that entity's identity to the Certificate.

Certification Authority (CA) means an entity trusted by one or more entities to create, assign or revoke Certificates.

CP/CPSis a publicly available document that details the QuoVadis PKI and describes the practices employed in issuing Certificates.

Certificate Chain means a chain of Certificates required to validate a Holder's Certificate back through its respective Issuing CA to the Root CA.

Certificate Policy means a Certificate policy adopted by an Issuing CA operating within the QuoVadis PKI that defines all associated rules and indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

Certificate Renewal is when all the identifying information and the Public Key from the old Certificate are duplicated in the new Certificate, but there is a different (longer) validity period.

Certificate Requester is a natural person who is employed by the Applicant, or an authorised agent who has iu09 Tc.il old Cer

Certificate Re-issuance is when a Subscriber registers for a new Certificate, but there is an opportunity to change the identifying information (e.g. new email address, new last name, etc.) or other information (corrected Certificate Policies, modified key usage, etc.) from what was in the old Certificate. The new Certificate also has a different Public Key and a different validity period from the old Certificate.

Certificate Re-key is when all the identifying information from the old Certificate is duplicated in the new Certificate, but there is a different Public Key and a different validity period.

Certificate Revocation means the process of removing a Certificate from the Portal and indicating that the Key Pair related to that Certificate should no longer be used.

Certificate Revocation List (CRL) means a list of Certificates signed by the Issuing CA that have been revoked.

Confirming Person is a natural person who must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) who has express authority to sign the QV Authority Letter on behalf of the Applicant.

Contract Signer is a natural person who is employed by the Applicant and who has express authority to sign the Subscriber Agreement on behalf of the Applicant.

Counterparty means a person that is known to a Nominating RA 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 RA is reliably able to identify the Counterparty through business records maintained by the RA 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 Certificate's Operational Term; is digitally signed by the Issuing CA; and (vi) has prescribed Key Usages and Reliance Factor that governs its issuance and use whether expressly included or incorporated by reference to this CP/CPS.

Digital Signature see Advanced Electronic Signature.

Digital Transmission means the transmission of information in an electronic format.

Device means software, hardware or other electronic or automated means configured to act in a particular way without human intervention.

Device Certificate means a Certificate issued to identify a Device. Distinguished Name means the unique identifier for the Holder of a Certificate.

eIDAS Regulation or eIDAS means Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

Enterprise RA means an employee or agent of an Organisation unaffiliated with the CA who authorises issuance of Certificates to that Organisation.

EU Qualified Certificate means Qualified Certificate as specified in the eIDAS Regulation.

Federal Information Processing Standards (FIPS) means the standards that deal with a wide range of computer system components including: hardware, storage media, data files, codes, interfaces, data transmission, networking, data management, documentation, programming languages, software engineering, performance and security.

Identify means a process to distinguish a subject or entity from other subjects or entities.

Identity means a set of attributes which together uniquely identify a natural person or entity.

Identification means reliance on data to distinguish and Identify a natural person or entity.

Individual means a natural person.

Internal Server Name means a Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Issuing CA means a subordinate CA duly authorised to operate by QuoVadis to issue Certificates to Subscribers within the QuoVadis PKI.

Issuing CA Agreement an agreement entered into between QuoVadis and an Issuing CA to provide Issuing CA services within the QuoVadis PKI.

Issuing CA Certificate A Certificate issued by a QuoVadis Root CA to an subordinate CA enabling that Issuing CA to issue Certificates to Subscribers.

Key means a sequence of symbols that controls the operation of a cryptographic transformation (e.g. Encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

Key Pair means two related Keys, one being a Private Key and the other a Public Key having the ability whereby one of the pair will decrypt the other.

National Competent Authority (NCA) means a national authority responsible for the regulation of payment services. The NCA approves or rejects authorisations for Payment Service Providers in its country.

Object Identifier means the unique identifier registered under the ISO registration standard to reference a specific object or object class.

Operational Term means the term of validity of a Certificate commencing on the date of its issue and terminating on the earlier of (i) the date disclosed in that Certificate or (ii) the date of that Certificate's Revocation.

Organisation means an entity that is legally recognised in its jurisdiction of domicile (and can include a body corporate or un-incorporate, partnership, trust, non-profit making Organisation, or Government entity).

Participants means participants within the QuoVadis PKI and include (i) Issuing CAs and their Subsidiaries and Holding Companies; (ii) RAs and their Subsidiaries and Holding Companies; (iii) Subscribers, (including Certificate Applicants); (iv) Authorised Relying Parties.

PKCS means Public-Key Cryptography Standard.

Policy Management Authority (PMA) means the QuoVadis body responsible for overseeing and approving CP/CPS amendments and general management.

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

Private Key means a Key forming part of a Key Pair that is required to be kept secret and known only to the

Qualified Certificate for Electronic Seal means a Certificate issued to a Legal Person (company) by a QTSP and is used to secure authenticity, integrity and confidentiality in electronic communication of messages and documents.

Qualified Electronic Signature means an Advanced Electronic Signature that is created by a Electronic SignatureQSCD and which is based on a Qualified Certificate for Electronic Signatures.

Qualified Electronic Signature/Seal Creation Device (QSCD) means an Electronic Signature/seal creation device that meets the requirements laid down in Annex II of the eIDAS.

Qualified Trust Service Provider (QTSP) means a trust service provider who provides one or more Qualified trust services and is granted the Qualified status under the eIDAS Regulation by the relevant supervisory body of an EU country.

QuoVadis means QuoVadis Limited, a Bermuda exempted company.

QuoVadis Issuing CA means QuoVadis in its capacity as an Issuing CA.

QuoVadis PKI means the infrastructure implemented and utilised by QuoVadis for the generation, distribution, management and archival of Keys, Certificates and Certificate Revocation Lists and the Repository to which Certificates and Certificate Revocation Lists are to be posted.

QuoVadis Root CA means QuoVadis in its capacity as a Root CA.

QSCD means Qualified electronic Signature/Seal Creation Device

Registration Authority means a RA designated by an Issuing CA to operate within the QuoVadis PKI responsible for identification and authentication of Subscribers.

RA Agreement an agreement entered into between an Issuing CA and a RA pursuant to which that RA is to provide its services within the QuoVadis PKI.

RA Certificate means a digital identifier issued by an Issuing CA (including QuoVadis in its capacity as an Issuing CA) in connection with the establishment of a RA within the QuoVadis PKI.

RA Officer means an Individual designated by a RA as bein

Root CA means QuoVadis as the source CA being a self-signed CA that signs Issuing CA Certificates.

Secure Cryptographic Device means device which holds the Subscriber's Private Key, protects this key against compromise and performs signing or decryption functions on behalf of the Subscriber.

Secure Signature Creation Device (SSCD) means a secure container specifically designed to carry and protect a Certificate, which meets the following requirements laid down in annex III of Directive 1999/93/EC:

1. Secure signature-creation