QuoVadis Root CA 1 G3

Version Control

Approved by	Date	Version	Comment
QuoVadis PMA	28 February 2002	2.05	ETA Revisions
QuoVadis PMA	01 August 2003	2.06	

1. INTRODUCTION

1.1. OVERVIEW

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that the QuoVadis PKI uses in the generation, issue, use, and management of Certificates and serves to notify Subscribers and Relying Parties of their roles and responsibilities concerning Certificates. This CP/CPS applies to the following Root CAs:

- QuoVadis an1. • QuoVadis an1.onoVedistie

responsibility and undertakes procedures to ensure

	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 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 Subscribers' 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 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 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. External Issuing CAs publicly-trusted must either be technically constrained, or undergo an independent audit and be publicly disclosed in the QuoVadis Repository.

also Section 9.6.1.

1.3.2. Registration Authorities and Other Delegated Third Parties

A Registration Authority (RA) is an entity that performs Identification and Authentication of Certificate Applicants, and initiates, passes along revocation requests for end user Subscriber Certificates, and approves applications for renewal or re-keying Certificates on behalf of an Issuing CA. QuoVadis and Issuing CAs may act as RAs for Certificates they issue.

RAs may be authorised by QuoVadis to delegate the performance of certain functions to third party validators if it meets the requirements of the QuoVadis CP/CPS. QuoVadis contractually obligates each RA and delegated third party to abide by the policies and industry standards that are applicable to their responsibilities. Where required by a Certificate Class, QuoVadis only allows the use of identity validation methods that have been approved by the relevant Supervisory Authority. Validation of Domains and IP Addresses for TLS and of email addresses included in Certificate Subject fields cannot be delegated.

Third parties, who enter into a contractual relationship with QuoVadis, may act as Enterprise RAs (ERAs) and

Subscribers are required to act in accordance with this CP/CPS and Subscriber Agreement. also Section 9.6.3.

1.3.4. Relying Parties

Relying Parties are entities that act in Reasonable Reliance on a Certificate and/or Digital Signature issued by QuoVadis. A Relying Party may, or may not, also be a Subscriber of the QuoVadis PKI. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the Certificate Status service is detailed within the Certificate.

Relying Parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. also Section 9.6.4.

1.3.5. Other Participants

Other Participants in the QuoVadis PKI are required to act in accordance with this CP/CPS and/or applicable agreements. Other participants include Accreditation Authorities such as Policy Management Authorities, Application Software Vendors, and applicable Community-of-Interest sponsors. Accreditation Authorities are granted an unlimited right to re-distribute QuoVadis CA 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

1.5. POLICY ADMINISTRATION

1.5.1. Organisation Administering The CP/CPS

This CP/CPS and related agreements and security policy documents referenced within this document are administered by the QuoVadis Policy Management Authority (PMA).

1.5.2. Contact Person

Enquiries or other communications about this CP/CPS should be addressed to the QuoVadis PMA.

Policy Director
QuoVadis Limited
11 Bermudiana Road, Suite 1640
Hamilton HM-08, Bermuda

Website: https://www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

Standards / Law	
	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security WebTrust for Certification Authorities – Extended Validation SSL WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates
SR 943.03 [ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen

Standards / Law	
Bermuda Authorised Certificate Service Provider	As defined in Bermuda's Electronic Transactions Act 1999
Application Software Vendor	Adobe Approved Trust List Technical Requirements, v.2.0 Apple Root Store Program Microsoft Trusted Root Store (Program Requirements) Mozilla Root Store Policy Chromium Project Root Store Certificate Policy

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

QuoVadis provides public repositories for its CA Certificates, revocation data for issued Certificates, CP/CPS, Terms and Conditions, and other important policy documents. The QuoVadis Repository is located at https://www.quovadisglobal.com/repository.

QuoVadis may register TLS Certificates with publicly accessible Certificate Transparency (CT) Logs. Once submitted, Certificate information cannot be removed from a CT Log.

QuoVadis' CA Certificates and its CRLs and OCSP responses are regularly accessible online with systems described in Section 5.

2.2. PUBLICATION OF CERTIFICATE INFORMATION

QuoVadis publishes a Repository that lists all Certificates that have been issued or revoked. Where a Certificate including an email address is issued, the Subscriber consents for the Certificate to be published in the Repository available for Relying Parties to download. The location of the Repository and OCSP responders

3. IDENTIFICATION A [illegible]

3.1.6. Recognition, Authentication, And Role Of Trademarks

Unless otherwise specifically stated in this CP/CPS, QuoVadis does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. QuoVadis may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2. INITIAL IDENTITY VALIDATION

isjEMC /H3 </MC1D 5 >>/DC /T10 1 Tf0.0001 Tc -0.002 Tw -31. -0 0 9.96 72 548.472Tm(3.2[(Y)c6-3.3 (i)-7 (r)3.7 -(t)6.d (n)2
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 Certificate in its sole discretion.

3.2.1. Method To Prove Possession Of Private Key

Issuing CAs shall establish that each Applicant for a Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the request for a Certificate. The Issuing CA shall do so in accordance wit (l)-2.2 (l)-2.1-0.0(l)-2.2 (l)-a40-9.2 (l)-daivte

When a subject:organizationIdentifer is included in Qualified or Regulated Certificates, the organizationIdentifer is formatted in accordance with Section 5.1.4 of ETSI EN 319 412-1.

3.2.2.1. Validation of Domain and Email Authorisation and Control

For each FQDN listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

i) BR Section 3.2.2.4.1 is no longer used as it is deprecated as of August 1, 2018;

ii) Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR Section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation);

iii)

v) 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;

vi) Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#Section-4, performed in accordance with BR Section 3.2.2.5.6; or

vii) BR Section 3.2.2.5.7 is not used by QuoVadis.

3.2.2.3. Wildcard [illegible]

i) Full name and legal status of the associated organisational entity;

ii) Any relevant existing registration information (e.g. company registration) of the organisational entity; and

iii) Evidence that the Subject is affiliated with the organisational entity which may include reference to an attestation or a Trusted Register. Attestations may be made by directors, executives, board members, or a natural person with authorisation duly delegated from another natural person in an authorised role.

The current validity must be established of any attestation or document regarding a natural person's relationship to a legal person. The role and authorisation of the natural person providing such attestation or document shall be recorded.

At least one digital or physical identity document shall be used as authoritative evidence. Identity documents must be valid at the time of proofing. Acceptable identity documents must contain a face photo and/or other information that can be compared with the Applicant's physical attributes. If physical identity documents are used as evidence, the documents shall be presented in their original form by the Subject of the identity proofing. If digital identity documents are used as evidence, only eMRTD (Electronic Machine Readable Travel Documents) according to ICAO 9303 part 10 and other digital documents that offer comparable reliability of the identity shall be accepted.

The Trusted Registers and identity documents (such as passports and

QuoVadis supports four levels of Remote Identity Verification:

Level	Description
RIV1	Base RIV plus manual review in defined cases (e.g, fraud risk, changes made by RA)
RIV2	Base RIV plus manual

3.2.5. Validation Of Authority

Where an Applicant's Name is to be associated with an Organisational Name to indicate his or her status as a Counterparty, Employee or specifies an Authorisation level to act on behalf of an Organisation, the RA will validate the Applicant's Authority by reference to business records maintained by the RA, its Subsidiaries, Holding Companies or Affiliates. Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in Appendix B. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

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

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.

QuoVadis maintains an internal database of previously revoked Certificates and previously rejected Certificate Requests. QuoVadis uses this information to identify subsequent suspicious Certificate Requests .

. Q(v)-i (u)e

4.2.1.1.

protected from unauthorised modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

4.3.2. Notification To Applicant Subscriber By The CA Of Issuance Of Certificate

QuoVadis may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, QuoVadis delivers instructions via email to the email address designated by the Subscriber during the application process.

4.3.3. Notification to NCA for PSD2 Certificates

QuoVadis maintains a register of NCA contact information. When a PSD2 Certificate is issued, QuoVadis will send a notification email to the NCA identified in the Certificate using the pre-registered contact information.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsible for installing the issued Certificate on the Subscriber's computer or cryptographic module according to the Subscriber's system specifications. A Subscriber is deemed to have accepted a Certificate when:

- The Subscriber downloads, installs, or otherwise takes delivery of the Certificate; or
- 30 days pass since issuance of the Certificate.

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 REASONABLE PRECAUTIONS TO PREVENT THE PRIVATE KEY'S LOSS, EXCLUSION, MODIFICATION, OR UNAUTHORISED USE.

4.4.2. Publication Of The Certificate By The CA

QuoVadis publishes all CA Certificates in its Repository. QuoVadis publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3. Notification Of Certificate Issuance By The CA To Other Entities

Issuing CAs and RAs within the QuoVadis PKI may choose to notify other entities of Certificate issuance.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key And Certificate Usage

The Certificate shall be used lawfully in accordance with the QuoVadis CP/CPS and Subscriber Agreement.

Subscribers are obligated to protect their Private Keys from unauthorised use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key And Certificate Usage

A Party seeking to rely on a Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. QuoVadis does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by QuoVadis are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the QuoVadis Repository.

A Relying Party should rely on a Digital Signature or TLS handshake only if:

i) the Digital Signature or TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,

ii) the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and

iii)

4.6.7. Notification of Certificate Issuance By The CA To Other Entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7. CERTIFICATE RE-KEY

Re-keying means creating a new Certificate with a new Public Key and serial number while keeping the Subject information the same.

4.7.1. Circumstance For Certificate Re-Key

Certificates may be re-keyed upon request. After re-

4.8.2. Who May Request Certificate Modification

QuoVadis modifies Certificates at the request of certain Certificate Subjects or in its own discretion. QuoVadis does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, QuoVadis verifies any information that will change in the modified Certificate. QuoVadis will only issue the modified Certificate after completing the verification process on all modified information. RAs are required to perform Identification and Authentication of all modified Subscriber information in accordance with the requirements of the applicable Certificate Profile.

4.8.4. Notification of Certificate Modification To Subscriber

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

4.8.5. Conduct Constituting Acceptance Of A Modified Certificate

Conduct constituting acceptance of a modified Certificate is in accordance with Section 4.4.1. Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate By The CA

QuoVadis publishes modified Certificates by delivering them to Subscribers. **4.8.5.**

vi) The NCA requests revocation for a PSD2 Certificate where the Subscriber (PSP) has lost its authorisation to act as a PSP or any PSP role in the Certificate has been removed (CRLReason #9, privilegeWithdrawn).

In the absence of exceptional circumstances confirmed with the relevant Supervisory Authority, QuoVadis will revoke a Certificate within 24 hours when QuoVadis becomes aware that a QSCD used for QCP-n-qscd or QCP-l-qscd loses its certification status.

QuoVadis may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days after receipt and c.422 -1.181 Td[(p)7.88 (a)-6.(d)-11. (2)4 rao (2)-1.3 (4)-1 Cy

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.

- SHA256WithRSAPSS
- SHA384WithRSAPSS
- SHA512WithRSAPSS
- PureEd25519

- A valid email address so that you can receive confirmation of your problem report and associated certificate revocations

QuoVadis will select the CRLReason code "keyCompromise" (value 1) upon discovery of such reason or as required by an applicable CP/CPS. Should a CA Private Key become compromised, the CA and all Certificates issued by that CA shall be revoked. QuoVadis provides additional instructions and support for keyCompromise at https://www.quovadisglobal.com/certificate-revocation/ and other resources as indicated in Section 1.5.2.1 of this CP/CPS.

4.9.13. Circumstances For Suspension

No suspension of Certificates is permissible within the QuoVadis PKI.

4.9.14. Who Can Request Suspension

No suspension of Certificates is permissible within the QuoVadis PKI.

4.9.15. Procedure For Suspension Request

No suspension of Certificates is permissible within the QuoVadis PKI.

4.9.16. Limits On Suspension Period

No suspension of Certificates is permissible within the QuoVadis PKI.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics Operational Characteristics

4.12. KEY ESCROW AND RECOVERY

QuoVadis provides optional Private Key Escrow services for certain Certificate Profiles (Appendix A, Section 10.1.2) under this CP/CPS. Private Key Escrow is only available if the Enterprise RA Administrator directs at the Account level. Private Key Escrow is prohibited for the following Certificate types:

- x CA Certificates
- x QV Advanced+ Certificates
- x QV Qualified Certificates
- x Any Certificate whose Private Key Usage is dedicated to Signing or Authentication
- x TLS Certificates
- x Codesigning Certificates

Private Key Escrow shall not be allowed when the nonRepudiation keyUsage is present in a Certificate as of version 4.32 of this CP/CPS.

4.12.1. Key Escrow And Recovery Policy And Practices

RAs are permitted to instruct QuoVadis to escrow the Subscriber's Encryption Private Key as specified in their RA Agreement. End-user Subscriber Private Keys shall only be recovered under the circumstances permitted within the RA Agreement and QuoVadis Portal administrator guide.

Escrowed Private Keys are stored in encrypted form using the QuoVadis Portal. Subscribers are notified when their Private Keys are escrowed. Properly authenticated Subscribers may subsequently retrieve their own Private Keys.

In addition, properly authenticated RA Officers with specific Key Recovery permissions may request retrieval of a Subscriber's Private Keys under the following conditions:

- RAs must protect Subscriber's escrowed Private Keys from unauthorised disclosure.
- RAs may retrieve Subscriber's escrowed Private Keys only for properly authenticated and authorised requests for recovery.
- RAs shall recover a Subscriber's escrowed Private Keys without the Subscriber's authority only for legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose.
- RAs must revoke the Subscriber's Key Pair prior to recovering the Private Key.
- RAs may not disclose or allow to be disclosed escrowed keys or archive key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organisation policy; or by order of a court of competent jurisdiction.
- RAs are not required to communicate any information concerning a key recovery to the Subscriber except when the Subscriber has requested recovery.

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Section o.8 ( )-lirhi

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

5.3.3. Training Requirements

QuoVadis provides relevant skills training in QuoVadis' PKI and TSA operations for the personnel performing information verification duties including:

i) basic PKI knowledge;
ii) software versions used by QuoVadis;
iii) authentication and verification policies and procedures;
iv) QuoVadis security principles and mechanisms;
v) disaster recovery and business continuity procedures;
vi) common threats to the validation process, including phishing and other social engineering tactics; and
vii) CA/Browser Forum Guidelines and other applicable industry and government guidelines.

QuoVadis logs the following events:

- CA Certificate and key lifecycle management events;
  - Certificate requests, renewal, and re-key requests, and revocation;
  - Approval and rejection of Certificate Requests;
  -

- Contractual obligations and other agreements concerning the operation of the CA
- System and equipment configurations, modifications, and updates
- Certificate request and verification
- Rejection or acceptance of a Certificate Request
- Certificate issuance, rekey, renewal, and revocation requests (and related actions)
- Certificate acceptance including Subscriber Agreements
- Escrow and retrieval requests
- Audit logs
- CA Key generation and destruction
- Appointment of an individual to a trusted role
- Destruction of a cryptographic module

5.5.2. Retention Period for Archive

5.6. KEY CHANGEOVER

Key changeove

	For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards. For Swiss Qualified Certificates of type QCP-n-qscd, and for Swiss Regulated Certificates, the Subscriber Private Keys are generated and stored on a QSCD. In the case that a QSCD used by QuoVadis for QCP-n-qscd or QCP-l-qscd loses its certification status, non-expired Certificates using the affected QCSD will be revoked. In some cases, a QTSP generates and manages Private Keys on behalf of the Subscriber. This is signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies. Section 10.1.1.

For Adobe Acrobat Trust List (AATL) Certificates, Subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 3.

QuoVadis never creates key pairs for publicly-trusted TLS Certificates and will not accept a Certificate Request using a Key Pair previously generated by DigiCert or QuoVadis. For publicly-trusted TLS Certificates, QuoVadis rejects a Certificate Request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 of CA/Browser Baseline Requirements or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

6.1.2. Private Key Delivery To Subscriber

Where QuoVadis generates Private Keys on behalf of the Subscriber, they are provided in a secure manner via the QuoVadis Portal (for example for S/MIME CereinS/MCID 13 >>BDC 652 0 Td5ica.1.1kitificlu S1eyaor eere Q3h E(ed)6.8U (

- 256-bit ECDSA Key or greater with the matching Secure Hash Algorithm version as required and a valid point on the elliptic curve; or
-

6.2.1. Cryptographic Module Standards And Controls

The generation and maintenance of the Root and Issuing CA Private Keys are facilitated through the use of HMS. The HSM used by Issuing CAs in the QuoVadis PKI are designed to provide at least FIPS 140-2 Level 3 and/or Common Criteria EAL 4 security standards in both the generation and the maintenance in all Root and Issuing CA Private Keys.

For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation.

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 unauthorised 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

	For EU Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a QSCD which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards. For Swiss Qualified Certificates of type QCP-n-qscd, and Swiss Regulated Certificates, the Subscriber Private Keys are generated and stored on a QSCD. In some cases, QuoVadis generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in Certificate policies. Section 10.1.1.

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 Usage Periods

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	12 to 36 months
TLS Certificates	398 days
All other Certificates	12 to 36 months

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day. For the purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximum requirements listed in Section 1.1 as applicable.

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 Public Key term or that exceeds the routine re-

QuoVadis personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CA/Browser Forum's Network Security Requirements and other relevant standards.

6.4.2. Activation Data Protection

If activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module. PINs may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the PIN. Activation Data should be memorised, not written down. Activation Data 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. Inactivity log out timeframes are set and enforced through internal information security policies and procedures to ensure security.

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 process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery 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 Qe.00toouy

(r) (a2 M)1.7 -1(ar.831

7.1.5.1. Name-Constrained serverAuth CAs

If the technically constrained Issuing CA Certificate includes the id-kp-serverAuth EKU, then it includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

i) For each dNSName in permittedSubtrees, QuoVadis confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements Section 3.2.2.4.

ii) For each iPAddress range in permittedSubtrees, QuoVadis confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

iii) For each DirectoryName in permittedSubtrees QuoVadis confirms the Applicant's and/or Subsidiary's Organisational name(s) and location(s) such that end entity Certificates issued from the Issuing CA will comply with Section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements.

If the Issuing CA is not allowed to issue certificates with an iPAddress, then the Issuing CA Certificate specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Issuing CA Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPvhe -1.1 (er)10.4 (o)386 -1.181 Td[(S)-2 (u)-6.2 (

x

Unless the keyCompromise is being used, superseded must be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- QuoVadis revoked the Certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, superseded must not be used.

7.2.1. Version Number

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

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR sha-384WithRSAEncryption [1 2 840 113549 1 1] OR sha-512WithRSAEncryption [1 2 840 113549 1 1 13] OR ecdsa-with-SHA256 [1 2 840 10045 4 3 2]

1 64Tm( )T(3)0.8 (2)-11.33.04 0.48 ref8 (1)0.68 f (64Tm( )T(3)0.8 (2)-11.33.04 0.48

7.4. LDAP PROFILE

QuoVadis hosts a Repository in the form of a Lightweight Directory Access Protocol (LDAP) directory for the purpose of (i) storing and making available all X.509 v3 Certificates issued under the QuoVadis PKI, (ii) facilitating public access to download these Certificates for Subscriber and Relying Party requirements, and (iii) receiving (from the QuoVadis PKI), storing and making publicly available, regularly updated CRL v2 information, for the purpose of Certificate validation.

7.4.1. LDAP Version Numbers

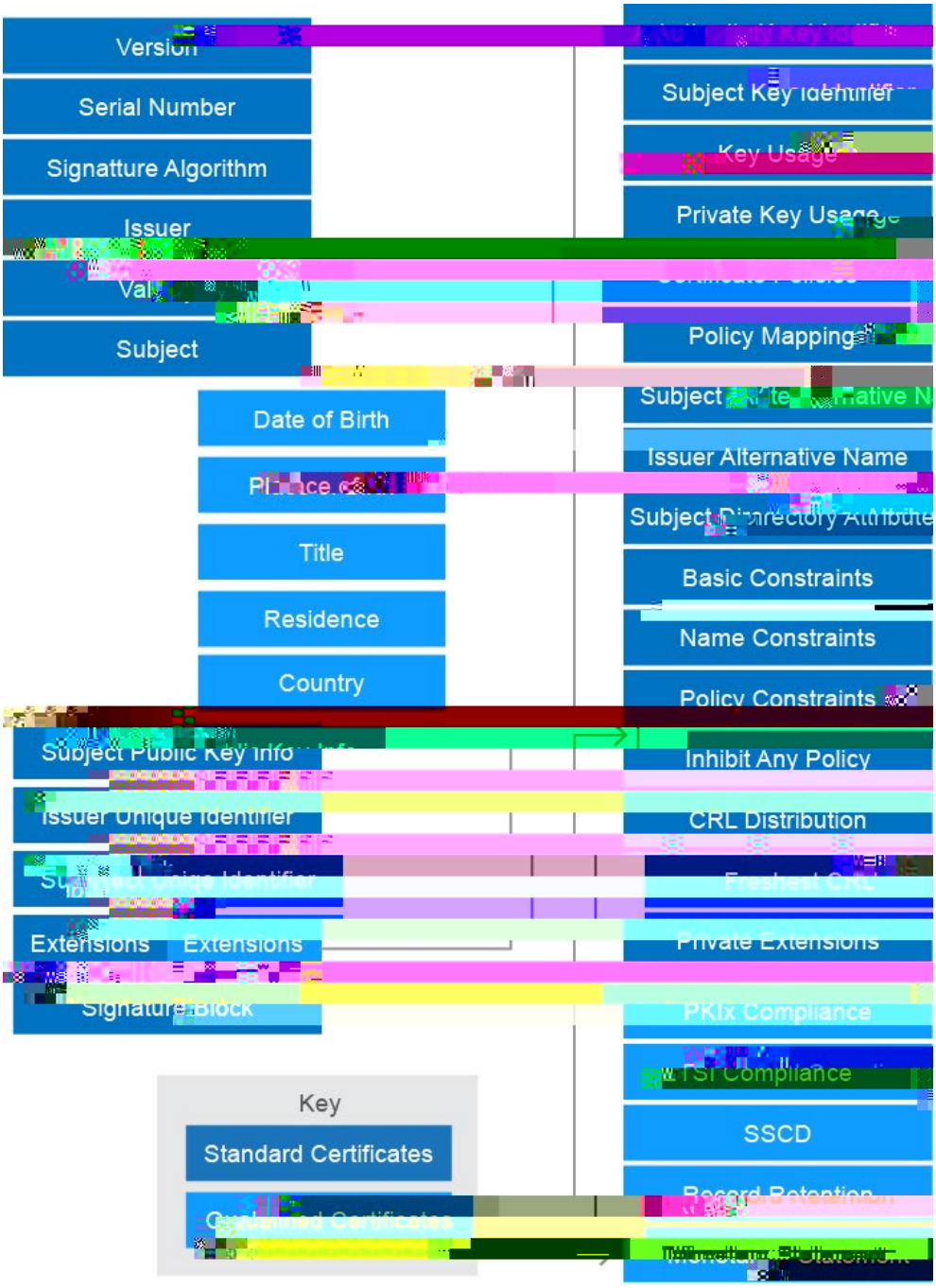
LDAP v3 in accordance with RFC 4510.

7.4.2. LDAP Extensions

Not applicable.

7.5. CERTIFICATE FIELDS AND ROOT CA CERTIFICATE HASHES

7.5.1. Certificate Fields



7.5.2. QuoVadis Root Certificate Hashes

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

7.5.2.1. QuoVadis Root CA 1 G3 Certificate Hashes

Field	**Certificate Profile**
Serial Number	78 58 5f 2e ad 2c 19 4b e3 37 07 35 34 13 28 b5 96 d4 65 93
Signature Block	Signature matches Public Key Root Certificate: Subject matches Issuer Key Id Hash (sha1): 92 ae ef 0e 89 02 ee 6d 79 68 d1 a1 0e 75 60 01 fa e4 eb fc Subject Key Id (precomputed): a3 97 d6 f3 5e a2 10 e1 ab 45 9f 3c 17 64 3c ee 01 Cert Hash(sha1): 1b 8e ea 57 96 29 1a c9 39 ea b8 0a 81 1a 73 73 c0 93 79 67

7.5.2.2. QuoVadis Root CA 3 Certificate

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance Or Renewal Fees

QuoVadis charges fees for verification, certificate issuance and renewal. QuoVadis may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

QuoVadis may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation Or Status Information Access Fees

QuoVadis does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. QuoVadis

Revocation EV 1.3.6.1.4.1.8024.0.2.100.1.3 1.3.6.1.4.1.8024.1.18 1 1 Tf 5.001 Tc -0.001 Tw 0.83 0 Td [(R)3 (e)

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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

QuoVadis follows the Privacy Notices posted on its website when handling personal information. https://www.quovadisglobal.com/privacy-policy which also includes privacy information for Remote Identity Verification. 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

9.5.1. Property Rights In Certificates And Revocation Information

QuoVadis retains all intellectual property rights in and to the Certificates and revocation information that it issues. QuoVadis and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. QuoVadis, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2. Property Rights In The CP/CPS

Issuing CAs acknowledge that QuoVadis retains all intellectual property rights in and to this CP/CPS.

9.5.3. Property Rights In Names

A Subscriber and/or Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate and Distinguished Name within any Certificate issued to such Subscriber or Applicant.

9.5.4. Property Rights In Keys And Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of QuoVadis and end-

v) Promptly (a) request revocation of a Certificate, cease using it and its associated Private Key, and notify QuoVadis if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (b) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

vi) For Remote Identity Verification, use the identity proofing software distributed by QuoVadis. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;

vii) Ensure that individuals using Certificates on behalf of an organisation have received security training appropriate to the Certificate;

viii) Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, including only installing TLS Server Certificates on servers accessible at the Domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent; and

ix) Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that QuoVadis notifies the Subscriber that the QuoVadis PKI has been compromised.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Parties Representations And Warranties

- the Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
- the Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- the Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Certificate being relied upon;
- the Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
- the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
- the identity of the Subscriber is displayed correctly by utilising trusted application software; and
- A(l)-8 (a)-7 (l)-.2 (at)6.6 (t611.9 .217s)-4.7

HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO QUOVADIS IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER QUOVADIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CP/CPS, MAY BE MADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER.

For Swiss Qualified Certificates, QuoVadis liability is in accordance with Articles 17, 18, 19 of ZertES.

For EU Qualified Certificates, QuoVadis liability is in accordance with Extract 37 and Article 13 of the eIDAS Regulation.

9.9. INDEMNITIES

9.9.1. Indemnification By QuoVadis

To the extent permitted by applicable law, QuoVadis shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an Certificate issued by QuoVadis, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (i) a valid and trustworthy Certificate as not valid or trustworthy or (ii) displaying as trustworthy (a) an Certificate that has expired or (b) a revoked Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2. Indemnification By Subscribers

To the extent permitted by law, each Subscriber shall indemnify QuoVadis, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including 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 acts; or (iv) Subscriber's misuse of the Certificate or Private Key. Tt m.2.2 (a)-7 (2ic).9 (r)10./ (o (u)-15.a)-7seM8ubscribtrgramentty i-sclud ditiona( )]T
rse (c)1.3 (t)6.6 (i)6.9 (v)4e (d)6.8 (i)6.9 (r)10.3 act ors oiersamr(o)6.9 (y)3.9e (s)2.

i) Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the

Customer is Domiciled in or the Services are:	Governing Law is laws of:	Court or arbitration body with exclusive jurisdiction:

9.16.2. Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of QuoVadis. Unless specified otherwise in a contact with a party, QuoVadis does not provide notice of assignment.

9.16.3. Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (Attorneys' Fees And Waiver Of Rights)

QuoVadis may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. QuoVadis' failure to enforce a provision of this CP/CPS does not waive QuoVadis' right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by QuoVadis.

9.16.5. Force Majeure

QuoVadis is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond QuoVadis' reasonable control. The operation of the Internet is beyond QuoVadis' reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting QuoVadis.

10. APPENDIX A

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 EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the OID 0.4.0.194112.1.3	ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)		Adobe AATL Approved
	QuoVadis Qualified Certificate not on a QSCD. Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
	QuoVadis Qualified Certificate not on a QSCD, where the device is managed by a QTSP. Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCP-l), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.460 ETSI policy identifier OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
QV Closed Community	Used for reliance by members of the Issuer community only. Policies are defined in the CP/CPS of the Issuing CA.			

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 /

10.2. QV STANDARD

Purpose		
Standard Certificates provide flexibility for a range of uses appropriate to their reliance value including S/MIME, electronic signatures, authentication, and encryption.		
Registration Process		
Validation procedures for QuoVadis Standard Certificates collect either direct evidence or an attestation from an appropriate and authorised source of the identity (such as name and organisational affiliation) and other specific attributes of the Subject. Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. Identity proofing may be conducted via enterprise records, physical presence; Remote Identity Verification (RIV1-4), reliance on electronic signature, or video verification.		
Attribute	**Values**	**Comment**
Subject	/CN (mandatory) (GN+SN or Pseudonate	

10.3. QV ADVANCED

Purpose
QV Advanced Certificates provide reliable verification of the Subject's identity and may be used for a broad range of applications including Digital Signatures, encryption, and authentication.
Registration Process

10.4. QV ADVANCED +

Purpose
QuoVadis Advanced+ Certificates are used for the same purposes as QuoVadis Advanced Certificates, with the

	1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	

Subjects may include an Organisation (legal person). Only methods approved for ZertES may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (RIV4 for NFC with RIV2 as a fallback option if NFC is not available), reliance on electronic signature, or video verification (in enrolments involving Financial Intermediaries).

Only a valid passport or national ID which allows entrance into Switzerland is accepted as evidence. Storage of personal data is in accordance with ZertES.

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

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)	0.4.0.194121.1.1 (optional semantics identifier OID that is included in QuoVadis Certificates)	Fixed

10.5. QV QU0.5.t2 0 0 9.901 Tc 0.00[Wm[1Td( )TJE)-6 (U).44Tw1[E.88 I7 (2 06 28.S0 9.901 Tc 0.00Tf-0.

organizationalIdentifier (optional)
/serialNumber (optional)
/E (optional)
/L (optional) /ST (optional) /C (mandatory)

If serialNumber is present then it must be structured per Section

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)	0.4.0.194121.1.1 (optional semantics identifier OID that is included in QuoVadis Certificates)	Fixed

10.5.2. eIDAS Qualified Certificate issued to a Natural Person

Purpose		
The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation. This type of QuoVadis Qualified Certificates does not use a QSCD for the protection of the private key. 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 2: Certificate profile for certificates issued to natural persons • ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements		
Registration Process		
Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for the "Policy for EU qualified certificate issued to a natural person" (QCP-n). QuoVadis recommends that QCP-n certificates are used only for electronic signatures. Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. Only methods approved for eIDAS Qualified Certificates may be used. Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, Remote Identity Verification (for Netherlands Qualified, RIV4 only; for Belgium Qualified, RIV4 for NFC with RIV2 as a fallback option if NFC is not available), or reliance on Qualified Electronic Signature. 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) = Natural Person (/GN+/SN or Pseudonym) /GN (mandatory if CN without Pseudonym) /SN (mandatory if CN without Pseudonym) Pseudonym (optional if natural person) /T (optional) /O (optional) /OU (optional) organizationalIdentifier (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:	See definitions in Section 7.1.1 Variable

	• 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 Certificate	/E	Optional

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

/E (optional)
/L (optional) /ST (optional) /C (mandatory)

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

10.5.4. eIDAS Qualified Certificate issued to a Legal Person elev0 (aaC)2.7 (t)6-6(p EE2-4 (T)8-(

Purpose

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 }

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) organizationalIdentifier (mandatory) /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	Variable

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 0.4.0.194112.1.1 (QCP-l) URL: https://www.quovadisglobal.com/repository	Fixed
Key Usage (Critical)	digitalSignature (optional) nonRepudiation	Variable
Extended Key Usage	clientAuth (optional) emailProtection (optional) documentSigning (optional)	Variable (at least one is present)
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 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

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-qcsd) URL: https://www.quovadisglobal.com/repository User Notice : qualified certificate	Fixed qcqcd

	/ST (optional) /C (mandatory)	
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 1.2.840.113612.5.2.2.1 IGTF Classic Authentication Profile 2.23.140.1.2.2 CABF OV	Fixed
Key Usage (Critical)	digitalSignature keyEncipherment dataEncipherment	Fixed
Extended Key Usage	clientAuth serverAuth	Fixed

10.8. QUOVADIS DEVICE

Purpose
QuoVadis Device Certificates are intended for a variety of uses including for Time-stamp Authority (TSA) applications. QuoVadis Device Certificates that have the serverAuth EKU comply with the CA/Browser

If the codeSigning EKU is present: = 2.23.140.1.2.3 If the timeStamping EKU is present, operated by QuoVadis: 1.3.6.1.4.1.8024.0.2000.6	
(1.3.6.1.4.1.11129.2.4.4) If the serverAuth EKU is present, this field MAY include two or more Certificate Transparency proofs from approved CT Logs.	Optional

Value
1 or 2 years expressed in UTC format. Effective September 1, 2020: maximum 397 days.
subject:organisationName (2.5.4.10)
subject:organisationUnit (2.5.6.5) Discontinued effective August 31, 2020.
subject:commonName (2.5.4.3) ch3e Common name s
subject:stateOrProvinceName (2.5.4.8)

	This field MAY include two or more Certificate Transparency proofs from approved CT Logs.

Purposes of Business SSL

QuoVadis Business SSL Certificates are intended for use in establishing web-based data communication conduits via TLS protocols. The primary purposes of a Business SSL Certificate are to:

- Identify the individual or entity that controls a website; and
- Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

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:

1 Tc -0.002 Tw 3.169 0 Td [(I)-2.3 (de)-7 (n)26.9 6-3 (iou)-3.3 (r)t-11.9 (S)1 (u)-3. (je)-7 .9 (c)-5.8 (t n)27(a)-7 (me)-7 (d)7 a thdercrtificate7-3.3

		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; digitalSignature (80)	