QuoVadis Root CA 1G3

QuoVadis Root CA 3/ QuoVadis Root CA 3 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: September24, 2021
Version: 4.35

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 Februaryem0		

QuoVadis PMA	2 August 2016	4.19	Updates for Regulation (EU) No 910/2014 (the eIDAS Regulation)
QuoVadis PMA	8 May 2017	4.20	Updates for the eIDAS Regulation; includes Legal Person Certificates. Updates for Code Signing Minimum Requirements
QuoVadis PMA	6 September 2017	4.21	Updates for CAA. Updates for submission of complaints
QuoVadis PMA	31 January 2018	4.22	Updates for the Baseline Requirements and Mozilla Root Store Policy
QuoVadis PMA	25 July 2018	4.23	Updates for Certificate Renewal. Additions in Appendix A relating to Qualified Certificate QSCD, where the device is managed by QuoVadis on behalf of the subject (1.3.6.1.4.1.8024.1.410).
QuoVadis PMA	30 July 2018	4.24	Updates for domain vetting (CA/B Forum Ballot 218)
QuoVadis PMA	7 December 2018	4.25	Updates to include changes for EU Qualified certs and itsme Sign Issuing CA G1. More explicit reference to the BR Domain Vetting methods
QuoVadis PMA	6 June 2019	4.26	Updates for where QSCD managed on behalf of Subscriber by QuoVadis . Updates to revocation requests. Updates for Baseline Requirements domain and IP address validation methods. Change to CRL update frequency
QuoVadis PMA	20 June 2019	4.27	Included PSD2 Qualified eSeal (QSealC) according to ETSI TS 119 495
QuoVadis PMA	23 August 2019	4.28	Adding QuoVadis responsibilities managing keys on behalf of the Subscriber. Clarifying revocation procedures
QuoVadis PMA	27 March 2020	4.29	Changes to comply with Mozilla Root Store Policy v2.7, CA/B Forum Ballot SC25, and clarifi est.76 Tm q 95.88.12 re Wt BT

Subscribers are required to act in accordance with this CP/CPS and Subscriber Agreement. *See* 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 C e a6 ( )Tj -0.001 Tc -0.002 Tw 0.217 0 Td [(a)-7 .8 (.)-0. d9 ( )]TJ (tu)-3

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

Private Key means the keyof a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to1 Td [(c Tf 9.9(r)10.4 yb)3.9 [57.309 710.55 417.9653 79c Tf 9.d d app>o 5.7 (a)-7etira6.

Standards / Law	
	WebTrust for Certification Authorities – Extended ValidationSSL WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates
SR 94303 [ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen

Standards / Law
Microsoft Trusted Root Store (Program Requirements) Mozilla Root Store Policy v.2.7

3.1. NAMING

3.1.1. Types Of Names

All Subscribers require a distinguished name that complies with the ITU X.500 standard for Distinguished Names(DN). The QuoVadis PMA approves naming conventions for the creation of distinguished names for Issuing CA applicants. Different naming conventions may be used by different Issuing CAs.

The Subject name of all Certificates issued to Individuals shall be the authenticated common name of the Subscriber. Each User must have a unique and readily identifiable X.501 DN. Alternatively, DNs may be based on domain name components, e.g. CN=John Smith, DC=QuoVadis, DC=BM. The Common Name may contain the applicant's first and last name (surname).

For Certificates issued under the Baseline Requirements, the use of Internal Server Names and Reserved IP Addresses is prohibited, and the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and/or the Subject Alternative Name extension.

The Distinguished Names of a Code Signing Certificate must identify the legal entity that intends to have control ove Tj -0.06 Tj -0.0t ide tnse of 0 9 Tj -0.0t ide rivatee oK when signing code.

3.1.2. Need For Names To Be Meaningful

QuoVadis uses Distinguished Names t identify bo Tj -0.0t the entity (i.se .s person, e atgam, device, s ors object) Tj -0.0t at is Tj -0.0t ide bject of the Certificati dend Tj -0.0t a identity tha at is the issers o.8 (0 9 Tj -0.3 (e)-6.9 (C)-4.3 (e)-7 (r)3.

3.1.3. Pseudonymous Subscribers

QuoVadis may issue pseudonymous nd entity Certificati de 0 9 Tj -0.0t ide are not proj -0.3 (i)-12.1 (b)3.8 (itide)6yd by policy applicable name space niqueness requirements are met. For Internationalised Domain Names (IDN), QuoVadis may include the P-33.8 (n)9.8 (y)3.9 (c)1.2 (o)6.9 (d)6.8 (e v)4 (er)10.4 (s)2.3 (i)6.9 (o)-5.2 (n)9.8 (o)6.9 (f)-4.3

3.1.4. Rules For Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness Of Names

The Subject Name of h Cstificati d]TJ 0 Tc 0 Tw 15.627 0 Td ( )Tj 0.006 Tc -0.009 Tw 0.217 0 Td [(i)6.9 (s)2.2 (s)2.3 (u)3.8 (

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 with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol, including PKCS#10. This requirement does not apply where a Key Pair is generated on behalf of a Subscriber

3.2.2. Authentication Of Organisation Identity

The Identity of an Organisation is required to be authenticated with respect to each Certificate that asserts (i) the identity of an Organisation; or (ii) an Individual or Device's affiliation with an Organisation. Without limitation to the generality of the foregoing, the Identity of any Organisation that seeks to act as a RA for its employees and/or employees of its respective Subsidiaries, Holding Companies or Counterparties is required to be authenticated.

In order to authenticate the Identity of an Organisation, at a minimum, confirmation is required that: (i) the Organisation legally exists in the name that will appear in the

ii) By sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response within a limited period of time that includes the Random Value to indicate that the Applicant controls that same email address.

QuoVadis maintains a list of High Risk Domains and has implemented technical controls to prevent the issuance of Certificates to certain domains. QuoVadis follows documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval.

QuoVadis uses a documented internal process to check the accuracy of information sources and databases to ensure the data is acceptable, including reviewing the database provider's terms of use. For EV, the approved sources are published in a file linked at https://github.com/digicert/reports/tree/master/validation-sources.

QuoVadis may include the Legal Entity Identifier (LEI) numbers in Certificates after verification through appropriate mechanisms, such as provided by Global Legal Enure Q5.8 (y).8 (.).0.4 (e p)7.8 (u)3916 0.006 Tc -0.006 TH4T

3.4.

For publicly-trusted TLS Certificates, Applicant information is required to include at least one FQDN or IP address to be included in the Certificate's SubjectAltName extension. QuoVadis implements documented procedures that require additional verifications as reasonably necessary for High Risk Certificate Requests prior to the Certificate's approval.

QuoVadis considers a source's availability, purpose, and reputation when determining whether a third-party data source is reasonably reliable. For TLS, QuoVadis does not consider a database, source, or form of identification reasonably reliable if QuoVadis or the RA is the sole source of the information.

4.2.1.1. Certificate Authority Authorisation (CAA)

Prior to issuing TLS Certificates, QuoVadis checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued. If the QuoVadis Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, QuoVadis processes the issue, issuewild, and iodef property tags as specified in RFC 8659. QuoVadis may not act on the contents of the iodef property tag. QuoVadis will not issue a Certificate if an unrecognised property is found with the critical flag.

CAA checking is optional for Certificates issued by a Technically Constrained Issuing CA as set out in Baseline Requirements Section 7.1.5, or where CAA was checked prior to the creation of a corresponding CT-p certificate that was logged in at least 2 public CT log servers.

DNS access failure can be treated as permission to issue when the failure is proven to be outside QuoVadis infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

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 containing those identifying domains as suffixes (e.g.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

Certificate issuance is governed by the practices described in and any requirements imposed by the CP/CPS. QuoVadis does not issue end entity TLS Certificates directly from its Root Certificates.

Certificate issuance by a Root CA requires a trusted role authorized by QuoVadis (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a Certificate signing operation. Databases and CA processes occurring during Certificate issuance are 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

QuoVadissw 2

4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate

Conduct constituting acceptance of a renewed Certificate is in accordance with Section 4.4.1.Issuct.3 (.3A)1.8 d.2p( )Tj E3.2 (t

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 formaw 0.94 0orpen se/LBody it(f)0.8 (or)c -0.00 (maw 8 (s)-)0.7 (p)-/LBody testenisten -4

QuoVadis may authorise the reissue of Certificates to Holders at no charge, unless the actions of the Holders were in breach of the QuoVadis CP/CPS or other contractual documents.

4.9.2. Who Can Request Revocation

Any appropriately authorised party, such as a recognised representative of a Subscriber or RA, may request revocation of a Certificate. QuoVadis may revoke a Certificate without receiving a request and without reason. Third parties may request revocation of a Certificate for problems related to fraud, misuse or compromise.

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 revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time Within Which The CA

4.9.8. Maximum Latency For CRL

CRLs for Certificates issued to end entity Subscribers are posted automatically to the online Repository within a commercially reasonable time after generation, usually within 10 minutes of generation. Regularly scheduled CRLs are issued at least once every 7 days and have a nextUpdate field value set to no more than 8 days beyond the thisUpdate field value.

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

Certificate status information is available via CRL and OCSP responder. For publicly-trusted TLS certificates, revocation entries on a CRL or OCSP Response are not removed until after the expiration of the revoked Certificate. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period, except for revoked Code Signing Certificates, which remain on the CRL for at least 10 years following the Certificate's validity period.

4.10.2. Service Availability

Certificate status services are available 24x7. QuoVadis operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

QuoVadis also maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

QuoVadis provides optional Private Key Escrow services for certain Certificate Profiles.

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 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.

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator/System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator/System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and

- audit, review, oversight, or reconciliation functions; and
-

granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates.

5.3.4. Retraining Frequency And Requirements

Employees must maintain skill levels that are consistent with QuoVadis' industry-relevant training and performance programs in order to continue acting in trusted roles. QuoVadis makes employees acting in trusted roles aware of any changes to QuoVadis' operations as necessary for them to perform their role. If QuoVadis' operations change, QuoVadis will provide documented training, in accordance with an executed training plan, to all employees acting in relevant trusted roles to those changes.

5.3.5. Job Rotation Frequency And Sequence

Not applicable.

5.3.6. Sanctions for Unauthorised Actions

QuoVadis employees and agents failing to comply with this CP/CPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied To Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP/CPS, applicable CA/Browser Forum standards, and other technical and operational documentation needed to maintain the integrity of QuoVadis' CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

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 (l)-7.1 (in)2.8 (6(d

Issuance of Certificates; and

Generation of CRLs and OCSP entries.

- Security events, including

  Successful and unsuccessful PKI system access attempts;

  PKI and security system actions performed;

  Security profile changes;

  Installation, update and removal of software on a PKI System;

  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 record;
- Identity of the entity making the journal record; and
- Details of the of record.

5.4.2. Frequency Of Processing Log

As required, generally within at least once every two months, a QuoVadis administrator reviews the logs generated by QuoVadis' systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (i) checks whether anyone has tampered with the logs, (ii) scans for anomalies or specific conditions, including any evidence of malicious activity, and (iii) if necessary, prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries may include recommendations to DigiCert's

5.5.2. Retention Period For Archive

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 Certificate. Detailed system generated logs are retained for 18 months based on a risk assessment

5.5.3. Protection Of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the PMA or as 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 an

event of a disaster, security compromise, or business failure. 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 CA Private Keys,

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

6.1.6. Public Key Parameters Generation And Quality Checking

QuoVadisusesCryptographic modules that conform to FIPS 186-2 and provide random value generation and on-board generation of Public Keys and a wide range of ECC curves.

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

Private Keys corresponding to QuoVadis Root Certificates are not used to sign Certificates except in the following cases:

i) Self-signed Certificates to represent the QuoVadis Root CA;

ii) Certificates for subordinate Issuing CAs and Cross Certificates;

iii) Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates), and

iv) Certificates for OCSP Response verification

Subscriber Certificates assert key usages based on the intended applicatiededOCedesoledefbii)± (Deda 0 Tdsesertifi2i97

6.2.2. Private Key (N of-M) Multi -Person Control

QuoVadis' authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. Backups of CA Private Keys are securely stored and require two-person access. Reactivation of a backed-up CA Private Key (unwrapping) requires the same security and multi person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

QuoVadis does not escrow its CA signature keys. QuoVadis may provide escrow services for end entity Subscriber Certificates in order to provide key recovery as described in Section 4.12.1.

6.2.4. Private Key Backup

QuoVadis Private Keys are generated and operated inside cryptographic modules which have been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. QuoVadis' CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process.

6.2.5. Private Key Archive

See Section 4.12. QuoVadis does not archive CA Certificate Private Keys.

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 pregenerates Private Keys and transfers them into a hardware token, for example transferring generated end-identity 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 TT1

QuoVadis documents and controls the configuration of its systems, including any upgrades or modifications made. Root Keys are kept

These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

QuoVadis Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

7.1.3. Algorithm Object Identifiers

QuoVadis Certificates are signed using one of the following algorithms or others as approved in accordance with Section 1.1:

sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
sha512WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]

7.2. CRL PROFILE

If present, this extension cannot be marked critical. This extension must be present for a Root CA or Issuing CA Certificate, including Cross Certificates. This extension may be present for Certificates not technically capable of causing issuance, subject to the requirement that the CRLReason cannot be unspecified (0) or certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. QuoVadis uses the following reasonCode values from RFC 5280

- keyCompromise(1)
- cACompromise (2)
- affiliationChanged (3)
- superseded(4)
- cessationOfOperation (5)

7.2.1. Version Number

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

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR sha-384WithRSAEncryption [1 2 840 113549 1 1 12] OR sha-512WithRSAEncryption [1 2 840 113549 1 1 13] OR ecdsa-with -sha256 [1 2 840 10045 4 3 2] 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
Issuer's Signature	[Signature]

7.2.2. CRL And CRL Entry Extensions

QuoVadis CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer certificate
Invalidity Date	Optional date in UTC format

/T1_0 1 Tf 0 Tc 0 4.2.2291 T2 2.47 0 Td ( )Tj-7

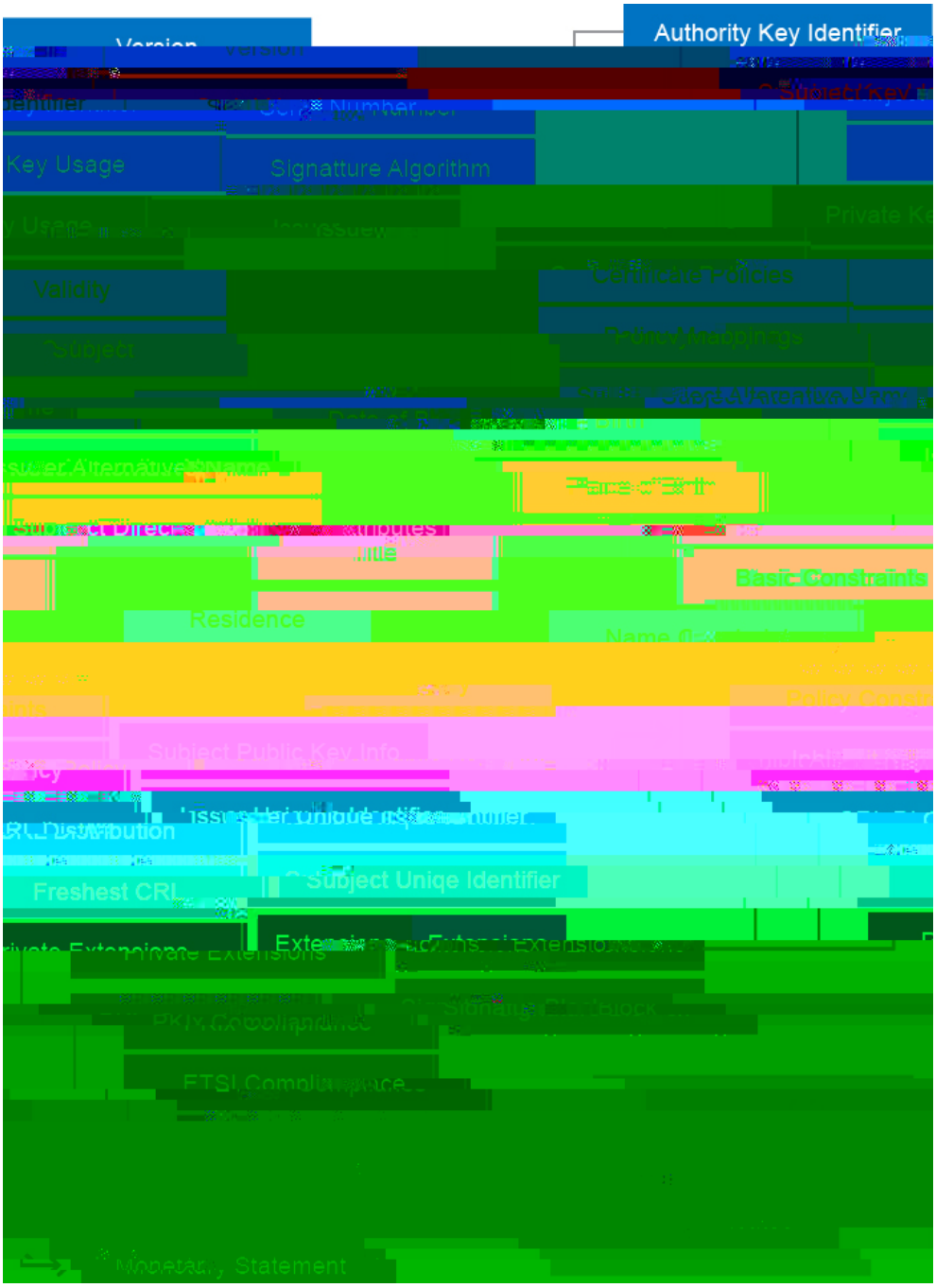
7.3. OCSP PROFILE

7.3.1. OCSP Version Numbers

The QuoVadis OCSP Responders conform to version 1, as defined by RFC 6960. If an OCSP response is for hpm osu3.8 (e)-pgT

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

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.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

QuoVadis follows the Privacy Notice 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

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 Private Key associated with a Certificate has been compromised in any way.

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

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 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.

9.10.3. Effect Of Termination And Survival

The conditions and effect resulting from termination of this CP/CPS will be communicated via the QuoVadis website upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

QuoVadis accepts notices related to this CP/CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from QuoVadis. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form

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

Customer is Domiciled in:	Governing Law is laws of:	Court or arbitration body with exclusive jurisdiction:
Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in the below city corresponding to the QuoVadis contracting entity listed in the Order Form. For QV CH: Zurich For QV NL: Amsterdam For QV DE: Munich For QVBE/DigiCert Europe Brussels For QV UK: London
Japan	Japan	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne
A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

9.15. COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to all applicable laws and regulations, including United States restrictions on the

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. See also Section 9.8.3 (Excluded Liability) above.

9.17. OTHER PROVISIONS

No stipulation.

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: 1.3.6.1.4.970uE		

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 enrolmentAgent	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				

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 forQuoVadis Standard Certificates collect either direct evidence or an attestation from a appropriate and authorised source, of the identity (such as name and organisational affiliation) and other specific attributes of the Certificate Holder.		
Attribute	Values	Comment
Subject	/CN (mandatory) (GN+SN or Pseudonym) /GN (mandatory if CNwithout Pseudonym) /SN (mandatory if CNwithout Pseudonym) Pseudonym (optional) /O (optional) /OU (optional) / serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory)	See definitions in Section7.1.1. Variable
SAN	/E	

Key Usage (Critical)

- Reference to a nationally recognized registration or other attributes which may be used to, as far a possible, distinguish the legal person from others with the same name.

If the Subscriberis 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 either held by the Subscriber or managed by QuoVadis and adhere to the following requirements:

- SecureCryptographic Device storage, preparation, and distribution is securely controlled by CA or RA;
- User activation datais 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) = Natural Person (/GN+/SN or Pseudonym) = Legal Person (/O) /GN (mandatory if CNwithout Pseudonym) /SN (mandatory if CNwithout Pseudonym) Pseudonym (optional) /O (optional) /OU (optional) /serialNumber (optional) /E (optional) /L (optional) /ST (optional) /C (mandatory)	See definitions in Section7.1.1 Variable
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+ Certificat 0.4.0.2042.1.2 ETSI NCP+ OID (optional)	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 (Critical)	digitalSignature (optional) nonRepudiation keyEncipherment (optional)	Variable
Extended Key Usage	clientAuth emailProtection documentSigning smartcardLogon	Variable (at least one is present)

10.4.1. Swiss Regulated Certificate issued to a Natural Person

Purpose
Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced-Certificate Class. They are issued out of Swiss Regulated CAs and have the notice text "regulated certificate" in the CertificatePolicies user notice. Swiss Regulated Certificates can be issued to natural and legal persons Swiss Qualified Certificates are described in the separate Section
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 Qualified Certificate. Evidence of the Subscriber's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence 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 A009 Tw -5.241 -1..7 ( )3 d [(E)- olecto2.2 (f)7..9 (d) Tw -5.2]TJ 024141 -1..7 arecse eqo

/T (optional)
/O (optional) /OU (optional)
/E (optional)
/L (optional) /ST (optional) /C (mandatory)

•

10.5. QV QUALIFIED - EIDAS

10.5.1. eIDAS Qualified Certificate issued to a Natural 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

Attribute	Values	Comment
Subject	/CN (mandatory) = Natural Person (/GN+/SN or Pseudonym) /GN (mandatory if CNwithout Pseudonym) /SN (mandatory if CNwithout 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); 3 character ISO 3166-1 [ISO 3166-1] country code of the country in which the identity document was issued; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); identifier (e.g. hash of the full name and birth date of the subject, or concatenation of name fragments and birth date, or a sequential number, or a random number) assigned by the CA to the subject.	

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 eBid	Fixed

id-

• Evidence that the Subscriber is associated with the organisational entity. 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) /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.	See definitions in Section 7.1.1 Variable
SAN	/E	Optional
Certificate Policies	1.3.6.1.4.1.8024.1.400 QV Qualified no QSCD, or 1.3.6.1.4.1.8024.1.401 QV Qualified no QSCD on behalf of 0.4.0.194112.1.0 (QCP-n) URL: https://www.quovadisglobal.com/repository	Fixed
Key Usage (Critical)	digitalSignature (optional) Nonrepudiation keyEncipherment (optional)	Variable
Extended Key Usage	emailProtection clientAuth documentSigning	Variable
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	

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	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 (id-etsi-qcs-semanticsId-Natural) (optional semantics identifier OID that is included in QuoVadis Certificates)	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 Certificate 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 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	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 0.4.0.194112.1.3 (QCP-l-qscd) URL: https://www.quovadisglobal.com/repository	Fixed
Adobe Acrobat Trust List	1.2.840.113583.1.1.9.1 Adobe Timestamp (link to TSA) 1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	Optional
Key Usage (Critical)	Nonrepudiation digitalSignature (optional)	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-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 cegJ ET QJ ET Q q ‹	

10.5.4. eIDAS Qualified Certificate issued to a Legal 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 Seals meeting the qualification requirements defined by the eIDAS Regulation. These Certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a legal person" (QCP-l). QuoVadis recommends that QCP-l 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 issued to a legal person" (QCP-l). The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified: I. by the physical presence by an authorised representative of the legal person; or II. 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 identified in association with this legal person that would appear in the organisation attribute of the Certificate, consistent with the national or other applicable identification practices. For the authorised representative of the legal 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. Additional steps to verify PSD2 specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA (e.g,, using a 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 paymiv 0.005a4.12 9dP 16 8 (ar1.94(ia)2.8 6)4.8 5(iv 0.005)TJ/TT1 1 8 (as(P)-403 (S)-6

- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorisation from an authorised Organisation representative; and
- Evidence that the Subscriber is associated with the organisational entity.

Private Keys for QV Swiss Qualified Certificates are generated and stored on a HSM or USB Token that meets the ZertES requirements, FIPS PUB 140-2, level 3 or EAL 4 standards. HSMs for QuoVadis Signing Services are located in QuoVadis datacentres. Access by the Subscriber to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone SSCD.

QV Swiss Qualified 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) /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.	See definitions in Section 7.1.1 Variable
SAN	/E	Variable
Certificate Policies	1.3.6.1.4.1.8024.1.4	

revocation if they can sufficiently prove compromise of the associated Private Key. Subscribers must request revocation as soon as possible. This should be within one working day after detection of loss or compromise of the Private Key pertaining to the Certificate, or if the data in the Certificate is no longer valid. Proxy Certificates will be supported in relation to Grid Certificate. A Grid Certificate must be revoked if a related Proxy Certificate is compromised in any way. The maximum Certificate Revocation List lifetime for Grid Certificates is 30 days.

Grid Certificate Re-Keying can only take place if the Subscriber is already in possession of a valid Grid Certificate and uses this Certificate to submit the Re-Key request. Certificates can only be Re-Keyed for up to a maximum of 3 years, after which period the Subscriber is required to apply for a new Certificate. If the Subscriber has lost their Private Key, or if their existing Certificate has expired, they will need to apply for new Certificate.

10.7.1.1. Grid End User Certificate

Purpose
Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid End User Certificate is to help the Subscriber to access the Grid services that require Certificate-based authentication.
Registration Process
The identity vetting of all Applicants must be performed by an approved RA. Face to face registration is required at the RA or alternatively the Applicants can have their identity vetted at a post office providing an approved identity vetting service. The Applicant must present a valid photo ID and/or valid official documents in accordance with formally documented RA procedures. The RA is responsible for recording, at the time of validation, sufficient information regarding the Applicant to identify the Applicant. The RA is responsible for maintaining documented evidence on retaining the same identity over time. The Certificate request submitted for certification must be bound to the act of identity vetting.
Digital Certific ate Delivery
All successful Grid End User Certificate requests will be processed by the QuoVadis Grid Issuing CA. QuoVac will not generate the Private Keys for Grid End User Certificates. If software tokens are used, the Private Key must be protected with a strong pass phrase that follows current best practices for choosing high-12.1 (f)0.8 (i11on)26To

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 Forum Baseline Requirements.
Registration Process

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) Discontinued effective August 31, 2020
Common Name	subject:commonName (2.5.4.3) cn = Common name
State or province (if any)	subject:stateOrProvinceName (2.5.4.8)
Country	subject:countryName (2.5.4.6)
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 – Same as Issuer's Subject Key Identifier
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	

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

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)	
Extended Key Usage	c=no; 1.3.6.1.5.5.7.3.3 (codeSigning)	
Field	Value	Comments

C 36 >>T319Q q o2actBT -0 -0 0 9.9

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 with this CP/CPS.

Step 1: The Applicant provides a signed Certificate Application to QuoVadis, which includes identifying information to assist QuoVadis in processing the request and issuing the Certificate, along with a PKCS#10 CSR and billing details.

Step 2: QuoVadis independently verifies information using a variety of sources in accordance with the "Verification Requirements" Sectionabove.

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 Code Signing Certificate. Step 7: The Certificate is delivered to the Applicant.