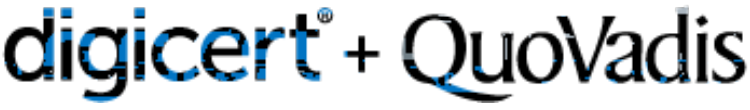
QuoVadis Root CA 1 G3

G3



Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement (CP/CPS) of QuoVadis Limited (QuoVadis), a company of DigiCert, Inc. It contains an overview of the practices and procedures that QuoVadis employs as a Certification Authority (CA). This document is not intended to create contractual relationships between QuoVadis Limited and any other person. Any person seeking to rely on Certificates or participate within the QuoVadis Public Key Infrastructure (QuoVadis PKI) must do so pursuant to a definitive contractual document. This document is intended for use only in connection with QuoVadis and its business.

This version of the CP/CPS has been approved for use by the QuoVadis Policy Management Authority

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 Root CA 1 G3
- QuoVadis Root CA 3 / QuoVadis Root CA 3 G3

QuoVadis maintains accreditations and certifications of its PKI. These include:

- Qualified Trust Service Provider (QTSP) under Regulation (EU) No. 910/2014 (eIDAS). QuoVadis is listed on the EU Trusted List (EUTL) for the Netherlands and for Belgium;
- Trust Service Provider under PKIoverheid in the Netherlands;
- Qualified Certification Service Provider in Switzerland (ZertES);
- WebTrust for CAs and WebTrust SSL Baseline with Network Security;
- Accredited CA by the EU Policy Management Authority for Grid Authentication in e-Science (EUGridPMA). This entitles QuoVadis to issue Certificates meeting the guidelines of the International Grid Trust Federation (IGTF); and
- Authorised Certification Service Provider (Bermuda) entitled to issue Accredited Certificates under the requirements of the Electronic Transactions Act 1999.

Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation. Other important documents include both private and public documents, QuoVadis' agreements with its customers, Relying Party agreements, and QuoVadis' privacy policies. QuoVadis may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for certificate and time-stamping services within the QuoVadis PKI. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation".

In addition, a *QuoVadis PKI Disclosure Statement* which summarises information about the QuoVadis PKI may be found in the QuoVadis Repository.

Where applicable, QuoVadis conforms to the current version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published at http://www.cabforum.org, and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Code Signing Baseline Requirements") published at https://aka.ms/csbr. In the event of any inconsistency between this CP/CPS and the normative provisions of the foregoing Applicable Requirements, then those Applicable Requirements take precedence over this document.

With the exception of CAs issuing Qualified Certificates in accordance with Swiss Regulations, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing CA and RA services within the QuoVadis PKI.

With the exception of CAs issuing Qualified Certificates in accordance with the European eIDAS Regulation, at QuoVadis' discretion, trustworthy parties may be permitted to operate Issuing CA and RA services within the QuoVadis PKI. Trust service components for EU Qualified Certificates may only be performed by QuoVadis-approved entities that have the relevant certifications. When trust service components are provided by another party QuoVadis maintains overall responsibility

and undertakes procedures to ensure that the security and functionality of the trust service meet the appropriate requirements.

1.2. DOCUMENT NAME, IDENTIFICATION AND APPLICABILITY

The Object Identifier (OID) assigned to QuoVadis is 1.3.6.1.4.1.8024. This CP/CPS applies to all CAs and Subscriber Certificatee.n681 TI/Cpached7v-7 ( )]TJ 0.003 Tw 12 -0 e( )T2 -0 e63e.n681 TI .T1d[(C)1i2 (.n681 TI)--74d( )Tj0.004

Certificate on a trusted system. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*. Within the QuoVadis Portal a Subscriber may also be referred to as *Certificate Holder*.

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 is detailed within the Certificate.

Relying Parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. *See* 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.

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

Standards / Law	
	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 Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016
SR 943.032 [VZertES] SR 943.032.1 [TAV]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016

3. IDENTIFICATION AND AUTHENTICATION

The Identification and Authentication procedures used by QuoVadis depend on the Class of Certificate being issued (*See* Appendix A and Appendix B). Issuing CAs may delegate the responsibility to one or more RAs.

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 over the use of the Private Key when signing code.

3.1.2. Need For Names To Be Meaningful

QuoVadis uses Distinguished Names that identify both the entity (i.e. person, organisation, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. QuoVadis only allows directory information trees that accurately reflect organisation structures.

3.1.3. Pseudonymous Subscribers

QuoVadis may issue pseudonymo9 0 Td[(t)6.6 (1 Tc 0FJ0 Tc 0 d 0.4a)-6.8 [(o)-5.2 (n)9.8 (ly)4 (allod(mo9a1.72 Tm63 0 Td[(is)-

3.2. INITIAL IDENTITY VALIDATION

QuoVadis

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) BR Section 3.2.2.4.3 is no longer used because it is deprecated as of May 31, 2019;

iv) Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorisation Domain Name (ADN). Performed in accordance with BR Section 3.2.2.4.4;

vi)

ii)

Level	Description
RIV1	Base RIV plus manual review in defined cases (e.g, fraud risk, changes made by RA)
RIV2	Base RIV plus manual review in all cases
RIV3	Base RIV plus NFC Authentication with manual review in defined cases (e.g, fraud risk, changes made by RA)
RIV4	Base RIV plus NFC Authentication with manual review in all cases

Base RIV may include OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options may include read of eMRTD data, Passive Authentication, and Active Authentication. Information collected and verified may include:

First name	ID number	ID issuance date
Last name	ID valid until	Issuing authority
Phone number	Scan of ID Document	Image of face
Email	Place of birth	Street
Date of birth	Nationality	Zipcode

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit A Certificate Application

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 i

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 CE]TJ0 Tc 2(C 0 Tdt51.4 (T)0.7 (H)w)1.9 (iSfb)10.8 (li)6.9 (s( )TjEMifh)2 (e)6 9 (

4.7. CERTIFICATE RE-KEY

i) QuoVadis obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;

ii) The Subscriber breached a material obligation under the CP/CPS or the relevant agreement

iii) QuoVadis confirms any circumstance indicating that use of a FQDN, IP address, or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);

iv) For code signing, the Application Software Vendor requests revocation and QuoVadis does not intend to pursue an alternative course of action;

v) For code signing, the Certificate is being used to sign Suspect Code;

vi) QuoVadis confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;

vii) QuoVadis confirms a material change in the information contained in the Certificate;

viii) QuoVadis confirms that the Certificate was not issued in accordance with the CA/Browser Forum requirements or relevant browser policy;

ix) QuoVadis determines or confirms that any of the information appearing in the Certificate is inaccurate;

x) QuoVadis right to issue Certificates under the CA/Browser Forum requirements expires or is revoked or terminated, unless QuoVadis has made arrangements to continue maintaining the CRL/OCSP Repository;

xi)

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

x) The Subscriber fails or refuses to comply, o (s)-4.a3.3 (uDC reW n,)-0.8 Attachet0.8somp o-7 (s)-4.os e s(th)-31ithbbeif

4.9.3. Procedure For Revocation Request

QuoVadis processes a revocation request as follows:

i) QuoVadis logs the request or problem report and the reason for requesting revocation based on the list in Section 4.9.1, including contact information for the requestor. QuoVadis may also include its own reasons for revocation in the log.

ii) QuoVadis may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).

iii) If the request is authenticated as originating from the Subscriber or an authorised party, QuoVadis revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.

iv) For requests from third parties, QuoVadis

iii) The number of Certificate problem reports received about a particular Certificate or Subscriber;

iv) The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

v) Relevant legislation.

The time used for the provision of revocation services is synchronised with UTC at least every 24 hours. Under normal operating circumstances, QuoVadis will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this Section and Section 4.9.1. For Certificates containing the ETSI OIDs defined in Section 10.1.1 the maximum delay between the receipt of the revocation request and the update of the Certificate Status information is at most 24 hours. For Certificates issued from the itsme sign Issuing CA, this 24 hour time period starts with the receipt of the revocation request at the itsme first-line helpdesk.

4.9.6. Revocation Checking Requirement For Relying Parties

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

4.9.7. CRL Issuance Frequency

QuoVadis uses its offline Root CAs to publish CRLs for its Issuing CAs at least every 6 months and within 18 hours after revoking an Issuing CA Certificate. QuoVadis updates the CRL for end-user Certificates at least every 12.5 hours and the date of the nextUpdate field will not be more than 72.5 hours after the date in the thisUpdate field.

Before revoking an Issuing CA Certificate a last CRL is generated with a nextUpdate field value of "99991231235959Z". The last CRL is available in accordance with Section 5.5.2. QuoVadis does not issue a last CRL until all Certificates in the scope of the CRL are either expired or revoked.

After the expiry date of an Issuing CA the most recent

nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

QuoVadis supports an OCSP capability using the GET method for Certificates. OCSP responders under QuoVadis' direct control respond with an "unauthorised" status for Certificates that have not been issued. QuoVadis may monitor its OCSP responders for requests for non-issued Certificates as part of its security response procedures.

4.9.11. Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements in Relation to Key Com9 (el)-3qis tNo51.4 -10 (. (oV)0.6 (a)-7 (dis)

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 (*see* 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:

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

•

5.1.5. Fire Prevention And Protection

QuoVadis datacentres are equipped with fire suppression mechanisms.

5.1.6. Media Storage

QuoVadis protects its media from accidental damage, environmental hazards, unauthorised physical access, and from obsolescence/deterioration during the period that records are required to be retained. Backup files are created on a daily basis. QuoVadis

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if QuoVadis, an Issuing CA, or RA is operating in accordance with this CP/CPS or approved registration procedures.

5.2.1.5. RA Administrators

RA Administrators manage the RA certificate management systems.

5.2.1.6. Security Officers

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

5.2.2. Number of Persons Required Per Task

QuoVadis requires that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating QuoVadis' Private Keys, generating a CA Key Pair, or backing up a QuoVadis Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification and Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure commensurate to their role

Without limitation, QuoVadis shall not be liable for employee conduct that is outside of their duties and for which QuoVadis has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.2. Background Check Procedures

QuoVadis verifies the identity of each employee appointed to a trusted role and performs a background check

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 Fole C3C /T /Artifact <</Atsp r619.614 -1.169 Td[.inta (c)-10.9 (s)-4.7 8 (ie)-7ct

d

- 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 log, (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 operations management committee and are made available to auditors upon request. QuoVadis documents any actions taken as a result of a review.

5.4.3. Retention Period For Audit Log

Audit logs relating to the Certificate lifecycle are retained as archive records for a period no less than eleven (11) years for Swiss Qualified Certificates and for seven (7) years for all other Certificates starting from the destruction of the CA Private Key or revocation or expiration of the Certificate. Certain high volume system generated logs are retained for 18 months based on a risk assessment. QuoVadis makes the audit logs available to auditors, as defined in Section 8, available upon request.

5.4.4. Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI. Only certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and vQl/]T17.7 (0.71 0 Td( )Tj.44.001 Tc -0.002 Tw 0.2170 Td[(Q)1.4 (u)-3.2 (C(t)6.7 e7 (p)-11.2 t(w)1.9 (8 (a-4.7 8.507 0 Td(. e4.

Based on the risk assessment, QuoVadis develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the Certificate data and management processes.

QuoVadis' audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of sys-5.8 (c)-ku8 (d)6.8f, rte ensitivipr41(g)-1 ((u)-3.2 (e)-7 (5.8

5.5.5. Requirements For Time-Stamping Of Records

QuoVadis supports time stamping of its records. All events that are recorded within the QuoVadis service include the date and time of when the event took place. This date and time are based on the system time on which the CA system is operating. QuoVadis uses procedures to review and ensure that all systems operating within the QuoVadis PKI rely on a trusted time source.

5.5.6. Archive Collection System

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

5.5.7. Procedures To Obtain And Verify Archive Information

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

5.6. KEY CHANGEOVER

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

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

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

5.7.4. Business Continuity Capabilities After a Disaster

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

5.8. CAAND/OR RATERMINATION

Unless otherwise addressed in an applicable agreement between QuoVadis and a counterparty, before terminating its CA or RA activities, QuoVadis may:

i)

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

QuoVadis CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony in the environments described in Section 5.1 and logged in accordance with Section 5.4. The cryptographic hardware is evaluated to FIPS 140-2 Level 3 and/or Common Criteria EAL 4 or higher. Hardware Security Modules (HSM) are always stored in a physically secure environment and are subject to security controls throughout their lifecycle. Activation of the hardware requires the use of two-factor authentication tokens. QuoVadis creates auditable evidence during the key generation process to prove that the CP/C2.2 (4)]TJ0 P.3 ((t)6.6 (w)-3.1 (o)]T8(t)6.6 (w).8 (t)ll.8 (t))-3.1 ()6.

6.1.3. Electronic Signature Public Key Delivery To Certificate Issuer

Subscribers generate Key Pairs and deliver Public Keys to the Issuing CA in a secure and trustworthy manner, such as submitting a CSR message to a QuoVadis Portal.

6.1.4. CA Public Key To Relying Parties

QuoVadis' Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root stores, and/or as roots signed by other CAs. All Accreditation Authorities supporting QuoVadis Certificates and all Application Software Vendors are permitted to redistribute QuoVadis CA Certificates.

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

6.1.5. Key Sizes

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

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

Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm if it is compliant with all applicable programs listed in Section 1.1. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

QuoVadis requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve alg 7.518 0 Td (n)2.78 02l (p)m84 0.337 0 Td[0 Td(-)Tj0.006(v)3.9 (e alg)6 (,11 T001 T

(y)-3 (C)-4.( )-3.2 (V)]H3J-0.001 T7 0.001 T/TT1 r otan83riK36.4ey UTw 12sf-2.4.3 (12g TcEMCe P)3.59(5)-2V5EMCg-ny CoV

(4TJ0.006)6.9 64 (y)-3 (C)-4.3 (5s)-4.7 (h)-3.3 (a)-7 (l)-7.1 (g)-1 (or)3.3 (i(A)-4.5 .8 (o)-122(r)3.4 (6 Tc -0.009 Tw -E7 (ta)-.7 (t

iii)

6.2.4. Private Key Backup

QuoVadis CA 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 .48 (u6)]3 (o)y TcTc6.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation And Installation

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

QuoVadis performs vulnerability scans of its networks at least once a quarter, and penetration tests at least annually.

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

6.8. TIME-STAMPING

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

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

QuoVadis uses the ITU X.509, version 3 standard to construct Certificates. QuoVadis adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. *See* Appendix A and Appendix B.

For publicly-trusted TLS Certificates, QuoVadis meets the technical requirements set forth in Sections 2.2,

7.1.5. Name Constraints

QuoVadis may include name constraints in the nameConstraints field when appropriate. For publicly-trusted TLS certificates, QuoVadis follows the requirements of Section 7.1.5 of the Baseline Requirements.

7.1.5.1. Name-

7.2. CRLPROFILE

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 requireme Tw -383t8-4.2 (e)-7 (368.671 0 Td( )Tj-0.001 Tc 0.001 Tw 0.217 0 Td (t)-

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 a Root CA or Issuing CA, including Cross Certificates, and that Certificate has been revoked, the revocationReason field within the RevokedInfo of the CertStatus is present and asserted.

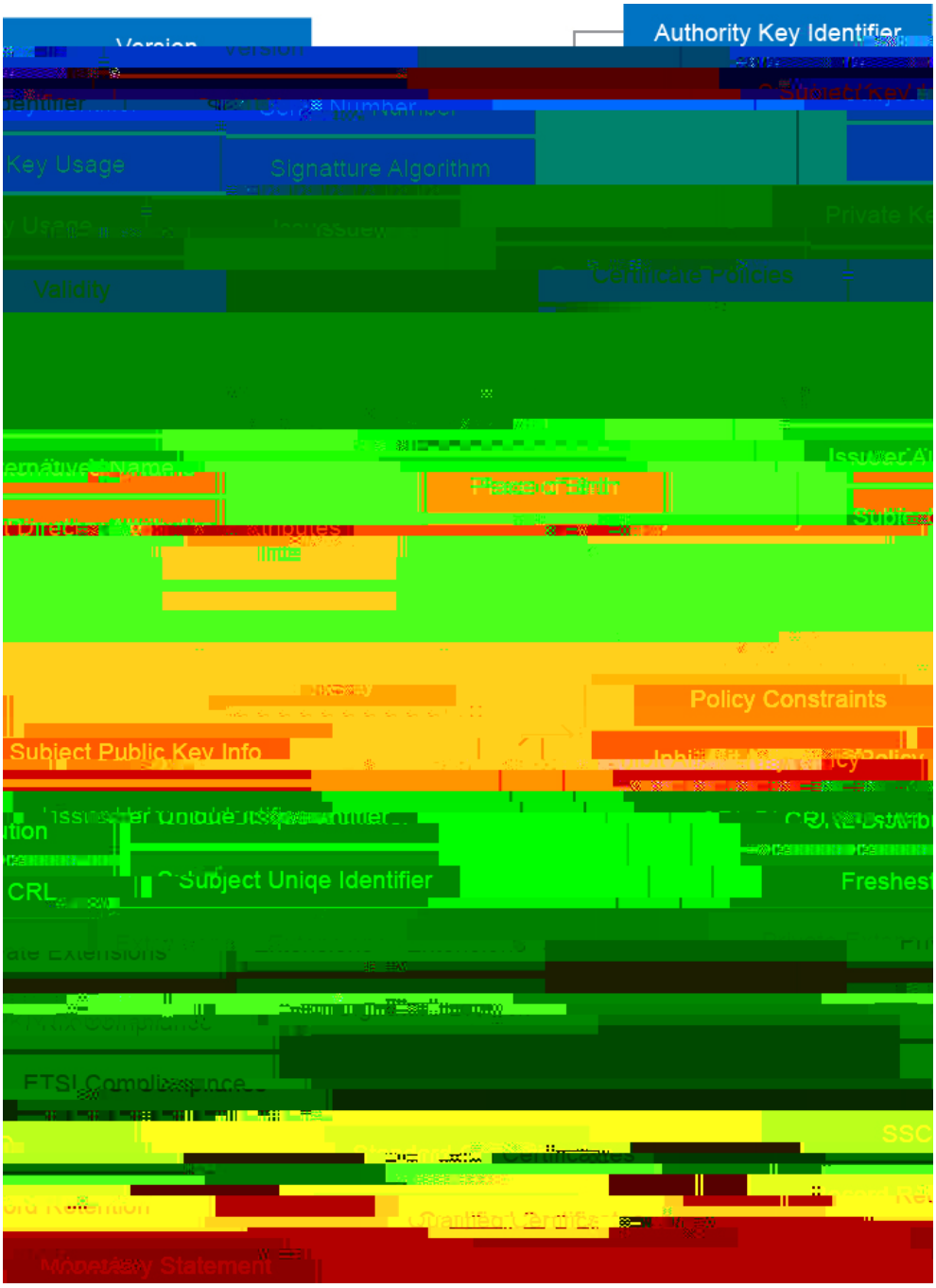
OCSP Responder Certificates have a maximum validity of 12 months.

7.3.2. OCSP Extensions

The singleExtensions of an OCSP response cannot contain the reasonCode (OID 2.5.29.21) CRL entry extension.ntry Tc 01o-7.5 ()13 0 T.3 (e]TJ.2 (n)2xJ-0.001 Tc 3.1 (n)-3jEMC /P.2 (.))0.81Toa(th)-3.2 (s) vesS8 (CSP)L38 (v)-3 (e)

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

8.2. IDENTITY AND QUALIFICATIONS OF ASSESSOR

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

Audits as applicaY9.96 -0 as appl0 (SSM)-3 (E)1 (N)0.9 (T)(T)]arphi arf,s rv anth1VTc 6.9 (c)-5di0.006 Tc9.8 (p)7.8 (l0 (SSM6.878

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 tertiCID 7 E1.5.578 0 D1.2 (h)3.8 (ar)o -0.00(li)6.90wion >>BDC BT9ar t4 (c)

9.4.

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.

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

QuoVadis provides test certificates for all types of Certificates.

9.6.2. RA Representations And Warranties

RAs represent and warrant that:

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

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

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

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

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

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

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

9.6.3. Subscriber Representations And Warranties

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorised. Subscribers are required to notify QuoVadis and any applicable RA if a change occurs that could affect the status of the Certificate.

QuoVadis requires, as part of the Subscriber Agreement or Terms of Us009 Twes

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.

- 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
- any alterations arising from security changes are identified by utilising trusted application software.

If the circumstances indicate a need for additional assurances, it is Relying Parties' responsibility to obtain such assurances. A Relying Party shall make no assumptions about information that does not appear in a Certificate. All obligations within this Section relate to Reasonable Reliance not

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

ii) Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

For Swiss Qualified Certificates such arbitration shall, unless agreed otherwise between the parties, take place in Switzerland.

For Qualified Certificates issued in accordance with eIDAS, arbitration for disputes related to financial or commercial matters will be dealt with in the country of the relevant QuoVadis entity named in the contract with the client. Arbitration for Certificate-related disputes will be dealt with in the country named in relevant QuoVadis Issuing CA Certificate.

9.14. GOVERNING LAW

The (i) laws that govern the interpretation, construction, and enforcement of this ATT2 (a)-7 (7 (t of)-e)-7 (r)3.3 ()3.4 (a)-4.7 r

10. APPENDIX A

10.1. CERTIFICATE PROFILES

Within the QuoVadis PKI an Issuing CA can only issue Certificates with approved Certificate Profiles. All Certificate Profiles within the QuoVadis PKI are detailed below.

Procedures for Subscriber registration as well as descriptions of fields are described below for each type of Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described in this CP/CPS may be drawn up under contract for individual Subscribers.

10.1.1. QuoVadis Certificate Class

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
QV Standard	Based on the ETSI Lightweight Certificate Policy (LCP), which has the policy identifier OID 0.4.0.2042.1.3	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.100 ETSI policy identifier OID: 0.4.0.2042.1.3 (optional)	Low	Optional
QV Advanced	Based on the ETSI Normalised Certificate Policy (NCP), which has the OID 0.4.0.2042.1.1. Features face-to-face (or equivalent) authentication of holder identity and organisational affiliation (if included).	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.200 ETSI policy identifier OID: 0.4.0.2042.1.1 (optional)	Medium	Optional
QV Advanced +	Similar to "QV Advanced" issued on an SSCD. Based on the ETSI Normalised Certificate Policy requiring an SSCD (NCP+), which has the OID 0.4.0.2042.1.2 Includes Swiss Regulated Certificates.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300 ETSI policy identifier OID: 0.4.0.2042.1.2 (optional)	High	Yes Adobe AATL Approved
QV Qualified	QuoVadis Qualified Certificate on a QSCD	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.400 ETSI policy identifier OIDs: 0.4.0.194112.1.2 (QCP-n-qscd) 0.4.0.194112.1.3 (QCP-l-qscd)	High	Yes Adobe AATL Approved
	QuoVadis Qualified Certificate on a QSCD, where the device is managed by a QTSP.	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.410	High	Yes

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

wher83.MC1188Qev Td(,)oC Td(d)9 re-10.711 a

QuoVadis Qualified
Certificate not on a QSCD,
where the device is managed

4.N-5.3 (d)3ID 28 >>BDC/P <</M CID 28 >>BDC q ref539.76 35.024 (1)-11.3 (2)0.8 (a)]TJ0 Tc 9 >>BDC Qq2

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			

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 physical presence; remote identity verification, reliance on eID or electronic signature, or video verification.

Attribute	**Values**	**Comment**

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

Validation procedures for QV Advanced Certificates are based on the Normalised Certificate Policy (NCP) described in ETSI EN 319 411-1.

Subjects may i m 16 >([(1)0.8 (.)]TJ)6ecy I4.6 d(-)Tj0.001 Tc -0.001.4 (i)1..337 0 Td[(1)0. 4.6 (16 >([(1)0.810. 4.6rc -0201.4

10.4. QV ADVANCED +

Purpose
QuoVadis Advanced+ Certificates are used for the same purposes as QuoVadis Advanced Certificates, with the only difference being that they are issued on a Secure Cryptographic Device. The QuoVadis Advanced+ Certificate Class is trusted in the Adobe Approved Trust List (AATL).
Registration Process

QuoVadis Advanced+ Certificates are based on with the Normalised Certificate Policy (NCP+) described in ETSI EN 319 411-1.

Subjects may include an Individual (natural person); an Organisation (legal person); or a natural person, device, or system identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, remote identity verification, or reliance on eID or electronic signature. AATL Certificates may use RIV1 or higher, ETSI Certificates may use RIV4 for NFC with RIV2 as a fallback option if NFC is not available.

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:

- Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA ordv:

	1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	
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)

SAN	/E 1.3.6.1.4.1.311.20.2.3 UPN	Variable
Certificate Policies	1.3.6.1.4.1.8024.1.300 QV Advanced+ Certificate 0.4.0.2042.1.2 ETSI NCP+ OID URL: https://www.quovadisglobal.com/repository User Notice: Regulated certificate	Fixed

These Certificates require a QSCD that meets the requirements laid down in Annex II of the eIDAS Regulation. The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.		
Attribute	**Values**	**Comment**
Subject	/CN (mandatory) = 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) 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: • 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 QSCD, or 1.3.6.1.4.1.8024.1.410 QV Qualified QSCD – on behalf of 0.4.0.194112.1.2 (QCP-n-qscd) URL: https://www.quovadisglobal.com/repository User Notice: Qualified certificate	Fixed Only 19.1.1VrepQ N

/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:

- 3 character identity type reference (e.g. PAS or IDC);
- 2 character ISO 3166 country code;
- hyphen-minus "

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 assurancaf241.44

Attribute	Values	Comment
Subject	/CN (mandatory) =/0 /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: • 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 • -	

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	

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

	• PSP identifier (authorisation number as specified by the NCA).	
SAN	/E	Variable
Certificate Policies	1.3.6.1.4.1.8024.1.450 QV Qualified – no QSCD 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 i	

	1.2.840.113583.1.1.9.2 Adobe Archive RevInfo (long term validation)	
Key Usage (Critical)	nonRepudiation	Fixed
Extended Key Usage	emailProtection documentSigning	Fixed
qcStatements		
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-1	esi4-qcStatement-1: Claim that the certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014	Fixed: issued before January 13, 2021
id-etsi-qcs-QcCClegislation (0.4.0.1862.1.7) id-etsi-qcs-7	esi4-qcStatement-7: Claim that the certificate is a Swiss Qualified Certificate (CH)	Fixed: issued after January 13, 2021
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.	

are accepted. Revocation requests can be made by end entities, RAs and QuoVadis. Others can also request 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.

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	Fixed
Key Usage (Critical)	digitalSignature keyEncipherment dataEncipherment	Fixed
Extended Key Usage	clientAuth emailProtection	Fixed

10.7.1.2. Grid Server Certificate

Purpose
Grid technology provides the software infrastructure for sharing of computing resources across various domains. The purpose of a Grid Server Certificate is to help secure communications with Grid servers.
Registration Process

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

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

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

Key Usage (Critical)	digitalSignature

11. APPENDIX B

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	c=yes; Digital Signature, Key Encipherment (a0)
Extended Key Usage	c=no; serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2)
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.1 } Certificate Policies; {2.23.140.1.2.2} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository
Certificate Transparency (optional)	(1.3.6.1.4.1.11129.2.4.4) 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.

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**
Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.200.1.1 } Certificate Policies; { 2.23.140.1.4.1 } [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository	1.3.6.1.4.1.8024.0.2.200.1.1 is the QuoVadis Code Signing OID. 2.23.140.1.2.3 is the Code Signing Baseline Requirements OID.
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =http://ocsp.quovadisglobal.com - id-ad-caIssuers (CA Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/<CA Name>.crt	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/<CA Name>.crl	

Purposes of Code Signing

The primary purpose of QuoVadis Code Signing Certificates is to establish that executable code originates

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

An Organisational Applicant is an Applicant that requests a Certificate subject other than the name of an individual. Organisational Applicants include private and public corporations, LLCs, partnerships, government entities, non-profit organisations, trade associations, and other entities.

Private Key Protection

Subscriber Key Pairs must be generated and protected in one of the following options:

- A Trusted Platform Module (TPM) that generates and secures a Key Pair and that can document the Certificate
- Holder's Private Key protection through a TPM key attestation
- A hardware cryptographic module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
- Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Verification Requirements

Before issuing a Code Signing Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to sign code in the name to be included in the Certificate.

Prior to issuing a Code Signing Certificate to an Organisational Applicant, QuoVadis:

i) Verifies the Applicant's possession of the Private Key;

ii) Verifies the Subject's legal identity, including any Doing Business As (DBA) as described in Section 3.2.2.2 of the Baseline Requirements,

iii) Verifies the Subject's address, and

iv) Verifies the Certificate Requester's authority to request a Certificate and the authentic10 1 Tf-(dd)-12.is, and