QuoVadis PMA	27 March, 2020	2.8	Changes to comply with Mozilla Root Store Policy v2.7, CA/B Forum Ballot SC25, revised Subscriber Agreement and Terms of Use, and change 5.92 80.88 63.6 re W n BTb1

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1. Overview 1
1.2. Document Name And Identification 2
1.3. PKI Participants 2
1.3.1. Certification Authorities 2
1.3.2. Registration Authorities 3
1.3.3. Subscribers 3
1.3.4. Relying Parties 3
1.3.5. Other Participants 3
1.4. Certificate Usage 4
1.4.1. Appropriate Certificate Uses 4
1.4.2. Prohibited Certificate Usage 4
1.5. Policy Administration ..... E

4.3.1. CA Actions During Certificate Issuance 18
4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate 18
4.4. Certificate Acceptance 19
4.4.1. Conduct Constituting Certificate Acceptance 19
4.4.2. Publication Of The Certificate By The CA 19
4.4.3. Notification Of CertificateIssuance By The CA To Other Entities 19
4.5. Key Pair And Certificate Usage 19
4.5.1. Subscriber Private Key And Certificate Usage 19
4.5.2. Relying Party Public Key And Certificate Usage 19
4.6. Certificate Renewal 20
4.6.1. Circumstance For Certificate Renewal 20
4.6.2. Who May Request Renewal 20
4.6.3. Processing Certificate Renewal Requests 20
4.6.4. Notification of New Certificate Issuance To Subscriber 20
4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate 20
4.6.6. Publication of the Renewal Certificate By The CA 20
4.6.7. Notification Of Certificate Issuance By The CA To Other Entities 20
4.7. Certificate ReKey 20
4.7.1. Circumstance for Certificate ReKey 20
4.7.2. Who May Request Certificate 20

e 202 Tf 0 Tc 0 Tw 11.04 -0 0 11.04 52/Span <</MCID 75 >>BDC T Tw 1 Tf 0 Tc 0 Tr 11 nce BDC MMTP ÞX>Ü ðÀ

4.12.1. Key Archival Escrow And Recovery Policy And Practices 27
4.12.2. Session Key Encapsulation And Recovery Policy And Practices 27
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 28
5.1. Physical Controls 28
5.1.1. Site Location and Construction 28
5.1.2. Physical Access 28
5.1.3. Power And Air-Conditioning 28
5.1.4. Fire Prevention And Protection 28
5.1.5. Media Storage 28
5.1.6. Waste Disposal 29
5.1.7. Off-Site Backup 29
5.2. Procedural Controls 29

f74 0 0 0 TT0 1 9 2 32 Tw 9 -0 0 9 144 584 4 Tm [(P)-10 3 (r)-4 42 Tm 49 73 72 (e)-1
tE51 0 11Bl 7 1

6.1.6. Public Key Parameters Generation And Quality Checking 37
6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field) 37
6.2. Private Key Protection And Cryptographic Module Engineering Controls 37
6.2.1. Cryptographic Module Standards And Controls 37
6.2.2. Private Key (N of M) Multi-Person Control 37
6.2.3. Private Key Escrow 38
6.2.4. Private Key Backup 38
6.2.5. Private Key Archive 38
6.2.6. Private Key Transfer Into Or From A Cryptographic Module 38
6.2.7. Private Key Storage On Cryptographic Module 38
6.2.8. Method Of Activating Private Key 38
6.2.9. Method Of Deactivating Private Key 38
6.2.10. Method Of Destroying Private Key 38
6.2.11. Cryptographic Module Rating 39
6.3. Other Aspects Of Key Pair Management 39
6.3.1. Public Key Archival 39
6.3.2. Certificate Operational Periods And Key Pair Usage Periods 39
6.4. Activation Data 39
6.4.1. Activation Data Generation And Installation 39
6.4.2. Activation Data Protection 39
6.4.3. Other Aspects Of Activation Data 40
6.5. Computer Security Controls 40
6.5.1. Specific Computer Security Technical Requirements 40
6.5.2. Computer Security Rating 40
6.6. Life Cycle Technical Controls 40
6.6.1. System Development Controls 40
6.6.2. Security Management Controls 41
6.6.3. Life Cycle Security Controls 41
6.7. Network Security Controls 41
6.8. Time-Stamping 41
7. CERTIFICATE, CRL, AND OCSP PROFILES 41
7.1. Certificate Profile 42
7.1.1. Version Number(s) 42
7.1.2. Certificate Extensions 42
7.1.3. Algorithm Object Identifiers 42
7.1.4. Name Forms 43
7.1.5. Name Constraints 43
7.1.6. Certificate Policy Object Identifier 43
7.1.7. Usage Of Policy Constraints Extension 44
7.1.8. Policy Qualifiers Syntax And Semantics 44
7.1.9. Processing Semantics For The Critical Certificate Policies Extension 44
7.2. CRL Profile 44
7.2.1. Version Number 44
7.2.2. CRL And CRL Entry Extensions 44
7.3. Online Certificate Status Protocol Profile 45
7.3.1. OCSP Version Numbers 45
7.3.2. OCSP Extensions 45
7.4. Certificate Transparency 45
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 45
8.1. Frequency, Circumstance And Standards Of Assessment 45
8.2. Identity And Qualifications Of Assessor 45
8.3. Assessor's Relationship To Assessed Entity 45
8.4. Topics Covered By Assessment 45
8.5. Actions Taken As A Result Of Deficiency 46
8.6. Publication Of Audit Results 46
8.7. Self Audits 46

9. OTHER BUSINESS AND LEGAL MATTERS 46
9.1. Fees 46
9.1.1. Certificate Issuance Or Renewal Fees 46
9.1.2. Certificate Access Fees 46
9.1.3. Revocation Or Status Information Access Fees 46
9.1.4. Fees For Other Services 46
9.1.5. Refund Policy 47
9.2. Financial Responsibilities 47
9.2.1. Insurance Coverage 47
9.2.2. Other Assets 47
9.2.3. Insurance Or Warranty Coverage For End-Entities 47
9.3. Confidentiality Of Business Information 47
9.3.1. Scope Of Confidential Information 47
9.3.2. Information Not Within The Scope Of Confidential Information 48
9.3.3. Responsibility To Protect Confidential Information 48
9.4. Responsibility To Protect Private Information 48
9.4.1. Privacy Plan 48
9.4.2. Information Treated As Private 48
9.4.3. Information Deemed Not Private 48
9.4.4. Responsibility To Protect Private Information 48
9.4.5. Notice And Consent To Use Private Information 48
9.4.6. Disclosure Pursuant To Judicial Or Administrative Process 48
9.4.7. Other Information Disclosure Circumstances 48
9.5. Intellectual Property Rights 49
9.5.1. Property Rights in Certificates and Revocation Information 49
9.5.2. Property Rights in the CP/CPS 49
9.5.3. Property Rights in Names 49
9.5.4. Property Rights in Keys and Key Material 49
9.5.5. Violation of Property Rights 49
9.6. Representations And Warranties 49
9.6.1. Certification Authority Representations 49
9.6.2. RA Representations and Warranties 50
9.6.3. Subscriber Representations And Warranties 50
9.6.4. Relying Parties Representations And Warranties 51
9.6.5. Representations And Warranties Of Other Participants 52
9.7. Disclaimers Of Warranties 52
9.8. Liability AND LIMITATIONS OF LIABILITY 52
9.9. Indemnities 53
9.9.1. Indemnification By QuoVadis 53
9.9.2. Indemnification By Subscribers 53
9.9.3. Indemnification By Relying Parties 53
9.10. Term And Termination 53
9.10.1. Term 53
9.10.2. Termination 53
9.10.3. Effect Of Termination And Survival 54
9.11. Individual Notices And Communications With Participants 54
9.12. Amendments 54
9.12.1. Procedure For Amendment 54
9.12.2. Notification Mechanism And Period 54
9.12.3. Circumstances Under Which OID Must Be Changed 54
9.13. Dispute Resolution Provisions 54
9.14. Governing Law 55
9.15. Compliance With Applicable Law 56
9.16. Miscellaneous Provisions 56
9.16.1. Entire Agreement 56
9.16.2. Assignment 56

9.16.3. Severability 56
9.16.4. Enforcement (Waiver Of Rights) 56
9.16.5. Force Majeure 56
9.17. Other Provisions 56
10. APPENDIX A – ROOT CA PROFILES 58
11. APPENDIX B 60
11.1. Business SSL 60

1.4. CERTIFICATE USAGE

For anyone listed in Section 4.9.2 of this CPS and the CA/Browser Baseline Requirements that requires assistance with revo

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

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

National Competent Authority: A national authority responsible for payment services. The NCA approves or rejects Authorisations for Payment Service Providers in its country.

Participants: A Participant is an individual or entity within the QuoVadis PKI and may include: CAs and their Subsidiaries and Holding Companies; Subscribers including Applicants; and Relying Parties.

Qualified Certificate: A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the qualification requirements defined by the applicable legal framework of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation") A Qualified Website Authentication Certificate is a TLS Certificate.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using the QuoVadis Repository.

Repository: The Repository refers to the CRL, OCSP, and other directory services provided by QuoVadis containing issued and revoked Certificates.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA. A Random Value is specified by QuoVadis and exhibits at least 112 bits of entropy.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA Also known as Issuing CA.

Subscriber: Means either the Individual to whom an end entity Certificate is issued or the Individual responsible for requesting, installing and maintaining the trusted system for which an TLS Certificate has been issued.

Subscriber Agreement: Is the agreement executed between a Subscriber and QuoVadis relating to the provision of designated Certificate related services that governs the Subscriber's rights and obligations related to the Certificate.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms and Conditions means the Master Services Agreement, Certificate Terms of Use, Privacy Policy and relevant QuoVadis CP/CPS. The Master Services Agreement references and makes the Certificate Terms of Use, Privacy Policy and relevant QuoVadis CP/CPS part of the Terms and Conditions. The itsme Issuing CA provides its own Terms and Conditions.

1.6.2. Acronyms

AND	Authorisation Domain Name
ALPN	TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737
CA	Certificate Authority or Certification Authority

CAA	Certificate Authority Authorisation
CP/CPS	Certificate Policy & Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
eIDAS	

Standards / Law	
	WebTrust for Certification Authorities – Extended ValidationSSL
	WebTrust for Certification Authorities –

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

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

2.2. PUBLICATION OF CERTIFICATE INFORMATION

QuoVadis publishes a Repository that lists all Certificates that have been issu

3.1.2. Need For Names To Be Meaningful

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 Authorization Domain Name (ADN). Performed in accordance with BR Section 3.2.2.4.4;

v) BR Section 3.2.2.4.5 is no longer used because it is deprecated as of August 1, 2018;

vi) BR Section 3.2.2.4.6 is no longer used because it is deprecated as of April 24, 2020;

vii) Confirming the Applicant's control over the requested ADN (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value

https://tools.ietf.org/html/draft- ietf-

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

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

At least one digital or physical identity document shall be used as authoritative evidence. Identity documents must be valid at the time of proofing. Tj -0.001 Tc -0.002-3.1 (e)-vi of of g 3.3 (s)-4ip(r)10.3 (d780r)1-6. of r5sta e(of)0.8 ( )

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

4.1.2. Enrolment Process And Responsibilities

Certificate Requests must be in a form prescribed by the Issuing CA and typically include i) an application form including all registration information as described by this CP/CPS, ii) secure generation of KeyPair and delivery of the Public Key to QuoVadis (a CSR may not be required), iii) acceptance of the relevant Subscriber Agreement or other terms of use upon which the Certificate is to be issued, iv) and payment of fees. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

A Certificate Request may be used for multiple Certificates to be issued to the same Applicant, (subject to the updating requirement in Section 4.2.1 of the TLS Baseline Requirements). The Certificate Request contains a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

All agreements concerning the use of, or reliance upon, Certificates issued within the QuoVadis PKI must incorporate by reference the requirements of this QuoVadis CP/CPS as it may be amended from time to time.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification And Authentication Functions

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 THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT. BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance For Certificate Renewal

Renewal means the issuance of a new Certificate to the Subscriber without changing the Subscriber or other participant's Public Key or any other information in the Certificate. QuoVadis may renew a Certificate if:

i) the associated Public Key has not reached the end of its validity period;

ii) the Subscriber and attributes are consistent; and

iii) the associated Private Key remains uncompromised.

QuoVadis may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. QuoVadis may notify Subscribers prior to a Certificate's expiration date. QuoVadis renewal requires payment of additional fees. QuoVadis may renew a certificate after expiration if the relevant industry permits such practices.

4.6.2. Who May Request Renewal

Only the Certificate Subject or an authorised representative of the Certificate Subject may request renewal of the Subscriber's Certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. QuoVadis will revalidate any information that is older than the periods specified in applicable standards for the Certificate Profile.

4.6.4. Notification of New Certificate Issuance To Subscriber

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

4.6.5. Conduct Constituting Acceptance Of

4.7.2. Who May Request Re-Key

QuoVadis will accept re-key requests from the Subject of the Certificate, an authorised representative for an Organisational certificate, or the nominating RA. QuoVadis may initiate a certificate re-key at the request of the Certificate Subject or at QuoVadis' own discretion.

4.7.3. Processing Certificate Re-Key Request

If the Private Key and any identity and domain information in a Certificate have not changed, then QuoVadis may issue a replacement Certificate using a previously issued Certificate or previously provided CSR. QuoVadis may re-use existing verification and authentication information in accordance with Section 3.3 unless QuoVadis believes that the information has become inaccurate.

4.7.4. Notification of Certificate Re-Key To Subscriber

QuoVadis may deliver the Certificate to the Subscriber in accordance with Section 4.3.1.

4.8.5. Conduct Constituting Acceptance Of A Modified Certificate

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

4.8.6. Publication Of The Modified Certificate By The CA

QuoVadis publishes modified Certificates by delivering them to Subscribers.

4.8.7. Notification Of Certificate Modification By The CA To Other Entities

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

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, QuoVadis and Issuing CAs verify that a revocation request was initiated by Subscribers, an RA, an Issuing CA, and other entities listed in Section 4.9.2 of this CP/CPS. Other parties may submit Certificate Problem Reports to QuoVadis to report reasonable cause to revoke the Certificate. Issuing CAs are required to provide evidence of the revocation authorisation to QuoVadis upon request.

4.9.1. Circumstances For Revocation

QuoVadis will revoke a Certificate within 24 hours after receipt and confirming one or more of the following occurred:

i) The Subscriber requests in writing that QuoVadis revoke the Certificate;

ii) The Subscriber notifies QuoVadis that the original Certificate Request was not authorised and does not retroactively grant authorisation;

iii) QuoVadis obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

iv) QuoVadis obtains evidence that the validation of domain authorisation or control for any FDQN or IP address in the Certificate should not be relied upon;

v) QuoVadis is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

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

vii) QuoVadis becomes aware that a QSCD used for QCP-qscd or QCP-l-qscd loses its certification status

QuoVadis may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days after receipt and confirming that one or more of the following occurred:

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) Revocation is required by the QuoVadis CP/CPS;

xii) QuoVadis confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed; or

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

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

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

ii)

iii) QuoVadis obtains evidence that the Issuing CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum Baseline Requirements or any Section of the Mozilla Root Store policy;

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

v) QuoVadis confirms that the CA Certificate was not issued in accordance with or that Issuing CA has not complied with the CP/CPS;

vi) QuoVadis determines that any of the information appearing in the CA Certificate is inaccurate or misleading;

vii) QuoVadis or the Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;

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

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

x) The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Vendors or Relying Parties.

In the event that an Issuing CA determines that its Certificate or the QuoVadis PKI could become compromised and that revocation of Certificates is in the interests of the PKI, following remedial action, QuoVadis may authorise the reissue of Certificates to Subscribers at no charge, unless the actions of the Subscribers 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 Certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

QuoVadis provides Anti-Malware Organisations, Subscribers, Relying Parties, Application Software Vendors, and other third parties (such as a National Competent Authority that issued the Authorisation Number in a PSD2 Certificate) with clear instructions on how they can report suspected Private Key compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates at https://problemreport.digicert.com/ and other resources listed in Section 1.5.2.1

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 personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

- the nature of the alleged problem;

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

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

4.9.13. Circumstances For Suspension

The QuoVadis PKI does not support suspension of Certificates.

4.9.14. Who Can Request

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 and access privileges are configured using the "least privileges" principle for the role. All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation Of Duties

Trusted roles requiring a separation of duties include those performing:

- authorisation functions such as the verification of information in Certificate Requests and certain approvals of Certificate applications and revocation requests,
- backups, recording, and record keeping functions;
- audit, review, oversight, or reconciliation functions; and
- duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, QuoVadis specifically designates individuals to the trusted roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. QuoVadis systems identify and authenticate individuals acting in trusted roles and restrict an individual from assuming multiple roles at the same time.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, And Clearance Requirements

The PMA is responsible and accountable for QuoVadis PKI operations and ensures compliance with this CP/CPS. Prior to the engagement of any person in the Certificate management process, QuoVadis verifies the identity and trustworthiness of such person. QuoVadis determines that all individuals assigned to trusted roles perform their prospective job responsibilities competently and satisfactorily as required.

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 prior to allowing such person to act in a trusted role. QuoVadis requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo. Background checks may include a combination of the following as required; verification of individual identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background.

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this Section cannot be met by QuoVadis due to a prohibition or limitation in local law, QuoVadis utilises a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

logs are protected in an encrypted format via a Key and Certificate generated especially for the purpose of protecting the logs.

5.4.5.

- CA Key generation and destruction
- Appointment of an individual to a trusted role
- Destruction of a cryptographic module

5.5.2. Retention Period For Archive

Audit logs relating to the certificate lifecycle are retained as archive records for a period of for seven (7) years. 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 maintain pAp 0 (as)24re[w 0.22p 0 (ae[w4 (o)-as)24re[wc 0 Tw isk ask 2-1.7 (t)6.6 A4e (nl0 T

access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing

This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, QuoVadis will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private KeySuch destruction shall be documented.

6.2.11. Cryptographic Module Rating

The cryptographic modules used by the QuoVadis PKI are validated to FIPS 140-2 Level 3 and/or Common Criteria EAL 4security standardsor higher.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key

different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the PIN. Activation Data should be memorised, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Subscriber's personal information.

6.4.3. Other Aspects Of Activation Data

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

6.5. COMPUTER SECURITY CONTROLS

QuoVadis has a formal Information Security Policy that documents the QuoVadis policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

6.5.1. Specific Computer Security Technical Requirements

QuoVadis secures its CA systems and authenticates and protects communications between its systems and trusted roles. QuoVadis' CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses. Inactivity log out timeframes are set and enforced through internal information security policies and procedures to ensure security.

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

QuoVadis' CA systems are configured to:

i) authenticate the identity of users before permitting access to the system or applications;

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

id-keyExchangeAlgorithm	[joint iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
	publicKeyType(2) 1]

7.1.4. Name Forms

Each Certificate includes a serial number that is unique to the Issuing CA. Optional subfields in the subject of an TLS Certificate must either contain information verified by QuoVadis or be left empty. TLS Server Certificates cannot contain metadata such as '-', '.' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable.

QuoVadis does not issue publicly-trusted TLS Certificates to a Reserved IP address or Internal Name.

For CA Certificates, the commonName attribute is present contains an identifier that uniquely identifies the CA and distinguishes it from other CAs. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. Issuer DNs meet the requirements in the CA/Browser Forum Baseline Requirements. See also Appendix A and Appendix B.

7.1.5. Name Constraints

QuoVadis may use nameConstraints when appropriate. For publicly-trusted TLS certificates, QuoVadis follows the requirements of Section 7.1.5 of the Baseline Requirements. If the technically constrained Issuing CA Certificates includes the id-kp-serverAuth EKU, then it includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

i) For each dNSName in permittedSubtrees, QuoVadis confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements Section 3.2.ts

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
Reason Code	Reason for revocation as described in Section 7.2
Issuing Distribution Point	Configured per RFC 5280 requirements, if included.

7.3. ONLINE CERTIFICATE STATUS PROTOCOL 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.

7.4. CERTIFICATE TRANSPARENCY

QuoVadis TLS Certificates MAY include Signed Certificate Timestamps (SCT) from independent CT Logs. Information on Certifi

9.1.5. Refund Policy

QuoVadis may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. FINANCIAL RESPONSIBILITIES

9.2.1. Insurance Coverage

QuoVadis maintains the following insurance related to its respective performance and obligations:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance Or Warranty Coverage For End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope Of Confidential Information

QuoVadis keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

i) Private Keys;

ii) Activation data used to access Private Keys or to gain access to the CA system;

iii) Business continuity, incident response, contingency, and disaster recovery plans;

iv) Other security practices used to protect the confidentiality, integrity, or availability of information;

v) Information held by QuoVadis as private information in accordance with Section 9.4;

vi) Audit logs and archive records; and

vii) Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS).

Any personal or corporate information held by Issuing CAs related to a Subscriber's application and the issuance of Certificates is considered confidential and will not be released without the prior consent of the

iv) For Qualified Certificates (a) if the policy requires the use of a QSCD, Electronic Signatures must only be created by a QSCD, (b) in the case of natural persons, the Private Key should only be used for Electronic Signatures, and (c) in the case of legal persons, the Private Key must be maintained and used under the control of the Subscriber and it should only be used for Electronic Seals.

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

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

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

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

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

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Parties Representations And Warranties

Relying parties are required to act in accordance with this CP/CPS and the Relying Party Agreement. A Relying Party must exercise Reasonable Reliance as set out in this Section.

i) Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by QuoVadis related to the Certificate or other

- the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
- 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 on the validity of a Digital Signature, not the accuracy of the underlying electronic record. Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations And Warranties Of Other Participants

Participants within the QuoVadis PKI represent and warrant that they accept and will perform any and all duties and obligations as specified by this CP/CPS.

9.7. DISCLAIMERS OF WARRANTIES

OTHER THAN AS PROVIDED IN SECTION 9.6.1, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, QUOVADIS DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. QUOVADIS DOES OTw 12 -NES

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 3i7Vw3 (.)-0.8 (-7 (n)-6.9

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

11. APPENDIX B

11.1. BUSINESS SSL

Field	Value
Version	V3
Serial Number	Unique number
Issuer Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)
Issuer Distinguished Name	Unique X.500 CA DN. CN = Variable O = QuoVadis Limited C = BM
Validity Period	397 days
Subject Distinguished Name	
Organization Name	subject:organisationName (2.5.4.10)
Organisation Unit	Not permitted in QuoVadis Business SSL.
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	

Verification of Country

11.2. EXTENDED VALIDATION SSL

Field	Value	Comments
Version		

	Certificate Policies; {2.23.140.1.1} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.quovadisglobal.com/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the QuoVadis Root CA 2 Certification Policies and Certificate Practice Statement.	
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.	
Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)	
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	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/QVSSLICA.crl or http://crl.quovadisglobal.com/qvsslg2.crl or http://crl.quovadisglobal.com/qvsslg3.crl	
cabfOrganizationIdentifier	cabfOrganizationIdentifier 2.23.140.3.1	Optional Refer to: CA/Browser Forum Ballot SC17

Purpose of EV SSL

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

- Identify the legal entity that controls a website;
- •

details requiring further explanation. QuoVadis procedures ensure that a second Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the EV Certificate and looks for discrepancies or other details requiring further explanation. Two QuoVadis Validation Specialists must approve issuance of the Certificate.

Step 7: QuoVadis creates the EV Certificate.

Step 8: The EV Certificate is delivered to the Certificate Requester.

QuoVadis may not issue an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that QuoVadis knows, or by the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, QuoVadis will decline the EV Certificate Request and notify the Applicant accordingly.

Renewal

Under the EV Guidelines, renewal requirements and procedures are generally the same as those employed for the validation and issuance for new Applicants. The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is thirteen months, except for the identity and authority of individuals identified in the EV Authority Letter.

In the case of outdated information, QuoVadis repeats the verification processes required by the EV Guidelines. If a company is no longer in good standing, or if any of the other required information cannot be verified, the Certificate is not renewed.

11.3.

attributes of the legal person, shall be verified 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. This may include via physical presence, Remote Identity Verification (RIV4 only), or reliance on a Qualified Electronic Signature.

11.4. QUOVADIS QCP-W-PSD2

ETSI TS 119 495 defines QWAC profiles and TSP policy requirements under the Payment Services Directive

Certificate in accordance with
Regulation EU No 910/2014

Note: PSP identifiers MAY contain hyphens, but Registration Schemes, ISO 3166 country codes, and NCA identifiers do not. Therefore if more than one hyphen appears in the final PSP identifier, the leftmost hyphen is a separator and the remaining hyphens are part of the PSP identifier.

PSD2 Roles

The NCA can assign one or more roles (RolesOfPSP) to payment service providers. QuoVadis also confirms the PSD2 role of the Certificate Applicant (RolesOfPSP):

11.5. CODE

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 Identifier 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. 2.23.140.1.4.1 is the Code Signing BaselineRequirements 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 (Certification Authority Issuer - 1.3.6.1.5.5.7.48.2); URL = http://trust.quovadisglobal.com/qvcscag1.crt	
CRL Distribution Points	c = no; CRL HTTP URL =http://crl.quovadisglobal.com/qvcscag1.crl	

Purposes of Code Signing

The primary purpose of QuoVadis Code Signing Certificates is to establish that executable code originates from a source identified by QuoVadis. QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the Certificate is actively engaged in doing business;
- That the Subject named in the Certificate complies with applicable laws;
- That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the Certificate.

Eligible Applicants

QuoVadis only issues Code Signing Certificates to Organisational Applicants and does not issue such certificates to Individual Applicants.

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

An Organisational Applicant is an Applicant that requests a Certificate subject other than the name of an individual. Organisational Applicants include private and public corporations, LLCs, partnerships, government entities, non-profit organizations, 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 Subscriber’s Private Key protection through a TPM key attestation

Organization Name	subject:organisationName (2.5.4.10)
Organisation Unit	Not permitted.
Common Name	subject:commonName (2.5.4.3) cn = Common name
Locality (if any)	subject:locality (2.5.4.6)
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)
Domain Components (DC)	DC=com, DC=quovadisglobal, DC=grid, DC=<organisation identifier>, DC=03=a6(g)3ITaE7 (44 2 287 isb)3IT 0 g03=p0.8 ()hde)Arti0