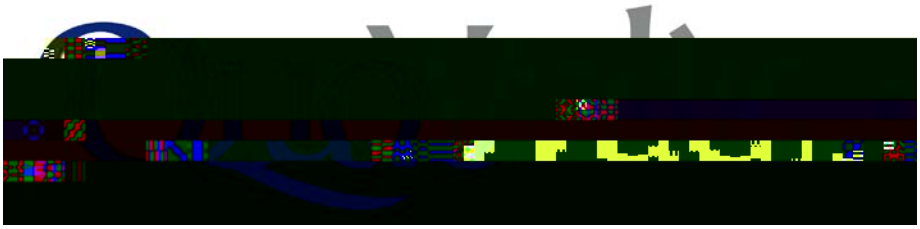


QUOVADIS ROOT CA2
CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT

Important Note About this Document

This document is the

Table of Contents

1. INTRODUCTION 1
1.1. Overview 1
1.2. Document Name And Identification 1
1.3. PKI Participants 1
1.5. Policy Administration 4
1.6. Definitions and Acronyms 4
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 5
2.1. Repositories 5
2.2. Publication of Certificate Information 6
2.3. Time or Frequency of Publication 6
2.4. Access Controls on Repositories 6
3. IDENTIFICATION AND AUTC5I(T)2(I)6(ON)1(A)8(N)1(( )Tj 04(t)-5()2(I)6(ON)1l 2MCI)6(OD.....)Tj (.....

1. INTRODUCTION

1.1. Overview

QuoVadis SSL Certificates are issued for use with the SSL 3.0/TLS 1.0 protocol to enable secure transactions of data through privacy, authentication, and data integrity.

QuoVadis Trusted Code Signing Certificates are used to provide users with reasonable assurance that the executable code they download comes from a source identified by QuoVadis.

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that QuoVadis Root CA2 uses in the generation, issue, use, and management of Certificates and serves to notify Certificate Holders and Relying Parties of their roles and responsibilities concerning Certificates.

QuoVadis ensures the integrity of its Public Key Infrastructure (PKI) operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between QuoVadis and any Participant in the QuoVadis PKI. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation.

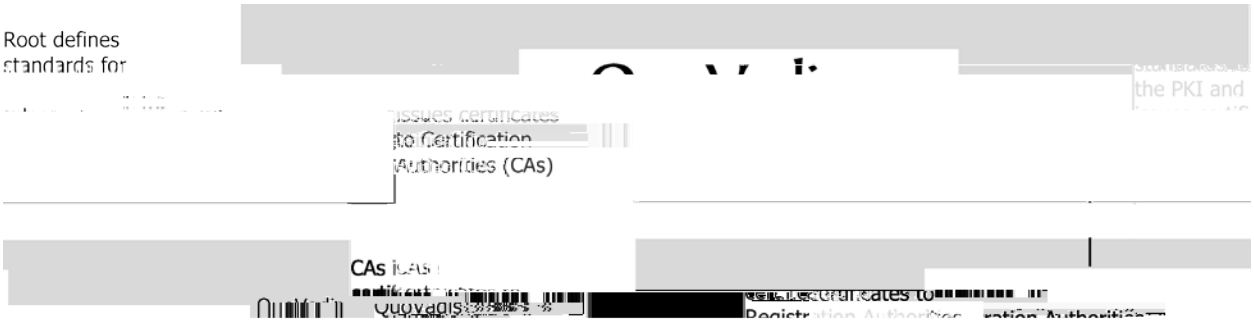
QuoVadis issues three forms of Certificates according to the terms of this CP/CPS:

i. Business SSL Certificates are Certificates for which limited authentication and authorization checks are performed on the Certificate Holder and the individuals acting for the Certificate Holder.

ii. Extended Validation SSL Certificates are Certificates issued in compliance with

- Registration Authorities ("RA") and Local Registration Authorities ("LRA");
- Certificate Holders including Applicants for Certificates prior to Certificate issuance; and
- Relying Parties.

The diagram below illustrates the components of the QuoVadis PKI:



1.3.1. Certification Authority

The following OIDs are pertinent to this CP/CPS:

QuoVadis Root CA2	1.3.6.1.4.1.8024.0.2
QuoVadis Global SSL ICA	1.3.6.1.4.1.8024.0.2.100.1
QuoVadis Business SSL	1.3.6.1.4.1.8024.0.2.100.1.1
QuoVadis Extended Validation SSL	1.3.6.1.4.1.8024.0.2.100.1.2
QuoVadis Trusted Code ICA	1.3.6.1.4.1.8024.0.2.100.2
QuoVadis Trusted Code Signing	1.3.6.1.4.1.8024.0.2.100.2.1

The inclusion of the QuoVadis Business SSL OID (1.3.6.1.4.1.8024.0.2.100.1.1) in the certificatePolicies extension of an end user certificate asserts adherence to and compliance with the Baseline Requirements.

The inclusion of the QuoVadis Extended Validation SSL OID (1.3.6.1.4.1.8024.0.2.100.1.2) in the certificatePolicies extension of an end user certificate asserts adherence to and compliance with the EV Guidelines.

QuoVadis Root CA2, the QuoVadis Global SSL ICA and the QuoVadis Trusted Code ICA issue Certificates to Certificate Holders in accordance with this CP/CPS. In its role as a CA, QuoVadis performs functions associated with public key

operations that include receiving requests; issuing, revoking and renewing a Certificate; and the maintenance, issuance, and publication of CRLs for users within the QuoVadis PKI. In its capacity as a CA, QuoVadis will:

- Conform its operations to this CP/CPS (or other relevant business practices);
- Issue and publish Certificates in a timely manner;
- Perform verification of Certificate Holder information in accordance with this CP/CPS;
- Revoke Certificates upon receipt of a valid request from an authorised person or on its own initiative when circumstances warrant; and
- Notify Certificate Holders of the imminent expiry of their Certificates.12(ev)-1(TJ -d -5(esr)-1-4(f)8.21(e i)(o)-2()-8(en)-8(t)--8(o)-

1.4.2. Prohibited Certificate Usage

QuoVadis Certificates may not be used and no participation is permitted in the QuoVadis PKI (i) in circumstances that breach, contravene, or infringe the rights of others; or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order; or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

No reliance may be placed on Certificates and Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use; (ii) in breach of this CP/CPS or the relevant Certificate Holder Agreement; (iii) in any

2.2. Publication of Certificate Information

QuoVadis operates and maintains its Repository with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the Certificates issued by its CAs.

QuoVadis publishes Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) resources to allow Relying Parties to determine the validity of a QuoVadis Certificate. Each CRL contains entries for all revoked un-expired Certificates issued. QuoVadis maintains revocation entries on its CRLs, or makes Certificate status information available via OCSP, until after the expiration date of the revoked Certificate.

2.3. Time or Frequency of Publication

QuoVadis issues a new CRL at least every twelve (12) hours and prior to the expiration of the current CRL. QuoVadis also provides an OCSP resource that is updated at least every twelve (12) hours. Certificate information is published promptly following generation and issue, and within 20 minutes of revocation.

2.4. Access Controls on Repositories

Participants (including Certificate Holders and Relying Parties) accessing the QuoVadis Repository and other QuoVadis directory resources are deemed to have agreed with the provisions of this CP/CPS and any other conditions of usage that QuoVadis may make available. Participants demonstrate acceptance of the conditions of usage of this CP/CPS by using a QuoVadis Certificate. Failure to comply with the conditions of usage of the QuoVadis Repository and web site may result in termination of the relationship between QuoVadis and the party, at QuoVadis' sole discretion, and any unauthorised

4.5. Key Pair And Certificate Usage

4.5.1. Certificate Holder Private Key And Certificate Usage

Certificate Holders shall protect their private keys from access by unauthorised personnel or other third parties. Certificate Holders shall use private keys only in accordance with the usages specified in the key usage field extension.

4.5.2. Relying Party Public Key And Certificate Usage

A Party seeking to rely on a Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement by querying the existence or validity of, or by seeking to place or by placing reliance upon, on a Certificate.

QuoVadis assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CP/CPS. QuoVadis does not warrant that any third party's software will support or enforce such controls or requirements, and all Relying Parties are advised to seek appropriate technical or legal advice.

Parties relying on a Certificate must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of the associated Certificate against the relevant CRL or OCSP resource provided by QuoVadis. Relying on an unverifiable digital signature or SSL/TLS session may result in risks that the Relying Party assumes in whole and which QuoVadis does not assume in any way.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS;
- That the Certificate is being used in accordance with its key usage field extensions specified in this CP/CPS and contained in the Certificate; and
- That the Certificate is valid at the time of reliance by reference to the QuoVadis CRL or OCSP and the Certificate has not been revoked.

Warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Renewal of a Certificate means reissuance of the Certificate using the same key pair. QuoVadis does not support Renewal; key pairs must always expire at the same time as the associated Certificate. QuoVadis makes reasonable efforts to notify Certificate Holders of the immindi

4.6. Certificate

4.6. Certificate 7870.867 0 -4(r)-6(s)1 .179 Ts-f1(m)368002 Tc

- QuoVadis

(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

QuoVadis maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.16. Limits On Suspension Period

The QuoVadis PKI does not support suspension of Certificates.

4.10. Certificate Status Services

Not applicable.

4.11. End Of Subscription

A Certificate Holder may terminate its subscription to the QuoVadis PKI by allowing a Certificate or applicable agreement to expire without renewal, or by voluntarily revoking a Certificate.

5.1.8. Off-Site Backup

An offsite location is used for the storage and retention of backup software and data. The off site storage is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e. software and data are stored in fire-rated safes and containers which are located behind access-controlled doors in areas accessible only by authorised personnel).

5.2. Procedural Controls

Administrative processes are described in detail in the various documents used within and supporting the QuoVadis PKI. Administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CP/CPS and other relevant operational documents. Except for certain RA functions described in this CP/CPS, QuoVadis does not outsource operations associated with Root CA2.

5.2.1. Trusted Roles

In order to ensure that one person acting alone cannot circumvent security, trusted responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy. This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of checks and balances to occur among the various roles.

5.2.2. Number Of Persons Required Per Task

- All aspects of the installation of new or updated software;
- All aspects of hardware updates;
- All aspects of shutdowns and restarts;
- Time and date of log dumps;
-

5.5.3. Protection Of Archive
Archives shall be retained and protected against modification or destruction.

5.5.4. Archive Backup Procedures
Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5. Requirements For Time-Stamping Of Records
QuoVadis supports time stamping of all 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 program 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.

5.5.7. Procedures To Obtain And Verify Archive Information
Only Issuing CA officers and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. QuoVadis may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their authorised representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval.

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

59(6.)]TJrLTw 8.893 0 Td [(s)-13(a)-1(f)o 9(6.)]TJrgke ica

- Give timely notice of revocation to each affected Certificate Holder.
- Revoke all Certificates that are still un-revoked or un-expired at the end of the notice period without seeking Certificate Holder's consent.
- Make reasonable arrangements to preserve its records according to this CP/CPS.
- Reserve its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary standards.
- Notify relevant government and accreditation bodies under applicable laws and related regulations or standards.

Upon termination of a CA, QuoVadis personnel shall destroy the CA private key by deleting, overwriting, or physical destruction.

6. TECHNICAL SECURITY CONTROLS
6.1. Key Pair Generation And Installation
6.1.1. Key Pair Generation

6.3.2. Certificate Operational Periods And Key Pair Usage Periods

The maximum validity periods for Certificates issued within the QuoVadis PKI are:

Root CA Certificate	25 years
Issuing CA Certificates	10 years
Business SSL Certificates	3 years
EV SSL Certificates	2 years

6.4. Activation Data

6.4.1. Activation Data Generation And Installation

Two-factor authentication shall be used to protect access to a private key. One of these factors must be randomly and automatically generated.

6.4.2. Activation Data Protection

No activation data other than access control mechanisms is required to operate cryptographic modules. Personal Identification Codes may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third party interception. Activation data should be memorized, not written down. Activation data must never be shared. Activation data must not contain the user's personal information.

6.4.3. O 0980 SCN 0.257 w /</MCID 16 .68 0 Td [(a)-1(t)-5(/TT1sc9w 12(3( )1(k)].1S-17)-5(i)-4(o3(a)4(

6.6.1. System Development Controls
Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2. Security Management Controls
Formal procedures and controls are in place to relating to the security-related configurations of QuoVadis' CA systems.

6.6.3. Life Cycle Security Controls
QuoVadis employs a configuration management methodology for the installation and ongoing maintenance of the CA systems. The CA software, when first loaded, provides a method for QuoVadis to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

The QuoVadis Chief Security Officer periodically verifies the integrity of the CA software and monitors the configuration of the CA systems.

6.7 Network Security Controls
All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

All unused network ports and services on Issuing CA equipment are turned off to provide protection against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone (offline) configurations.

6.8. Time-Stamping
See Section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES
7.1. Certificate Profile
7.1.1. Version Numbers
Information for interpreting Certificate and CRL Profiles may be found in IETF RFC 5280. QuoVadis Certificates follow the ITU X.509v3 standard, which allows a CA to add certain Certificate extensions to the basic Certificate structure.

7.1.2. Certificate Extensions
See Appendix A and Appendix B.

7.1.3. Algorithm Object Identifiers
See Appendix A and Appendix B.

7.1.4. Name Forms
See Appendix A and Appendix B.

7.1.5. Name Constraints
See Appendix A and Appendix B.

7.1.6. Certificate Policy Object Identifier
An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a CP/CPS such as this. The Certificate Policy OIDs that incorporate this CP/CPS into a given Certificate by reference (and identify that this CP/CPS applies to a given Certificate containing the OID) are listed in Appendix A and Appendix B.

7.1.7 Usage Of Policy Constraints Extension
Not applicable.

7.1.8. Policy Qualifiers Syntax And Semantics
QuoVadis Certificates include a brief statement in the Policy Qualifier field of the Certificate Policy extension to inform potential Relying Parties on notice of the limitations of liability and other terms and conditions on the use of the Certificate, including those contained in this CP/CPS, which are incorporated by reference into the Certificate.

7.1.9. Processing Semantics For The Critical Certificate Policies Extension
No stipulation.

7.2. CRL Profile
7.2.1. Version Number
QuoVadis issues version 2 CRLs conforming to RFC 5280, and which contain the basic fields listed below:

Version
Issuer Signature Algorithm
Issuer Distinguished Name
thisUpdate (UTC format)
nextUpdate (UTC format – thisUpdate plus 12 hours)
Revoked Certificates list
Serial Number
Revocation Date (see CRL entry extension for Reason Code below)
Issuer's Signature

7.2.2. CRL And CRL Entry Extensions
CRL Number (monotonically increasing integer - never repeated)
Authority Key Identifier (same as Authority Key Identifier in Certificates issued by CA)
CRL Entry Extensions
Invalidity Date (UTC - optional)
Reason Code (optional)

7.3. Online Certificate Status Protocol Profile
OCSP is enabled for all Certificates within the QuoVadis PKI.

7.3.1. Online Certificate Status Protocol Version Numbers
OCSP Version 1, as defined by RFC 2560, is supported within the QuoVadis PKI.

7.3.2. Online Certificate Status Protocol Extensions
No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1. Frequency, Circumstance And Standards Of Assessment
The practices specified in this CP/CPS have been designed to meet or exceed the requirements of, and QuoVadis is audited for compliance to, generally accepted and developing industry standards including:

- AICPA/CICA WebTrust for Certification Authorities and the WebTrust Extended Validation Program;
- Bermuda Authorised Certification Service Provider standards of the Bermuda electronic Transactions Act;
- Swiss Zert ES Qualified Certification Service Provider standards (ZertES), including adherence to

8.3. Assessor's Relationship To Assessed Entity

QuoVadis and the auditors do not have any other relationship that would impair their 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

Topics covered by the annual audits of QuoVadis include but are not limited to CA business practices disclosure (i.e., this CP/CPS), the service integrity of QuoVadis' CA operations, the environmental controls that QuoVadis implements to ensure trustworthy systems, and QuoVadis' compliance with relevant laws, regulations, and guidelines.

8.5. Actions Taken As A Result Of Deficiency

Actions taken as the result of deficiency 4(n)-8(c)-12(l)-4(u)-( )1(b)-13(e)(e)-13(su)(n)f)-21( )1(tpu)1(t)-5(h)-2f 0 Td ( )i

9.4.4. Responsibility To Protect Private Information

Information supplied to QuoVadis as a result of the practices described in this CP/CPS may be covered by national government or other privacy legislation or guidelines. QuoVadis will not divulge any private personal information to any third party for any reason, unless compelled to do so by law or competent regulatory J 0.00ci (n)-8(yo)-10(r)-6(a)-w o r-0(a)othe

QuoVadis' liability to any person for damages arising under, out of or related in any way to this CP/CPS, Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. QuoVadis shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whethe

liability per Digital Certificate per year (irrespective of the number of claims per Digital Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Digital Certificate in any one year of that Digital Certificate's life cycle.

9.9. Indemnities

Any user of a QuoVadis Certificate, whether a Certificate Holder, Relying Party or otherwise, shall indemnify and hold harmless QuoVadis from any and all damages and losses arising out of: (i) use of the QuoVadis Certificate in a manner not authorised by QuoVadis; (ii) tampering with the QuoVadis Certificate; or (iii) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional. In addition, Certificate Holders shall indemnify and hold harmless QuoVadis from any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a QuoVadis Certificate relating to: (i) Certificate Holder's breach of its obligations under the Certificate Holder Agreement or this CP/CPS; (ii) Certificate Holder's failure to protect its private key; or (iii) claims (including without

APPENDIX A – Root and Issuing CA Profiles

QuoVadis Root CA2

Field	Value
Version	V3
Serial Number	Unique number 0509
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Validity Period	25 years expressed in UTC format NotBefore: 11/24/2006 2:27 PM NotAfter: 11/24/2031 2:23 PM
Subject Distinguished Name	CN = QuoVadis Root CA 2 O =QuoVadis Limited C = BM
Subject Public Key Information	Public Key Algorithm: Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA Algorithm Parameters: 05 00 Public Key Length: 4096 bits
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; KeyID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b Certificate Issuer: Directory Address: CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM Certificate SerialNumber=05 09
Subject Key Identifier	c=no; 1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Key Usage	c=no; Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	c=yes; Subject Type=CA Path Length Constraint=None
Key Id Hash(sha1):	73 97 82 ea b4 04 16 6e 25 d4 82 3c 37 db f8 a8 12 fb cf 26
Cert Hash(md5):	5e 39 7b dd f8 ba ec 82 e9 ac 62 ba 0c 54 00 2b
Cert Hash(sha1):	ca 3a fb cf 12 40 36 4b 44 b2 16 20 88 80 48 39 19 93 7c f7

QuoVadis Global SSL ICA

Field	Value
Version	V3
Serial Number	Unique number 057a
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Root CA 2 O =QuoVadis Li875 /P <it(e)7(i)-6 667.08002h41l481 (a)3(d2 0 Td ( )Tj EMC3)-6 667.0p3ot C624 5 Issue

Appendix B – Certificate Holder Certificate Profiles

Business SSL

Field	Value
Version	V3

Certificate Policies	c=no; Certificate Policies; {1.3.6.1.4.1.8024.0.2.100.1.1 } [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.
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

Purposes of Business SSL

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

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

QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. As such, Certificates are not intended to provide any assurances, or otherwise represent or warrant:

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

Eligible Applicants

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

Verification Requirements

Before issuing a Business SSL Certificate, QuoVadis performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and has accepted a Certificate Holder Agreement for the requested Certificate.

Documentation requirements for organisation Applicants may include:

- Certificate of Incorporation (or analogous document); or
- Memorandum of Association (or analogous document); or
- Articles of Incorporation (or analogous document); or
- Business License (or analogous document); or
- Any power of attorney or other authority pursuant to which this Application has been signed.

Government and not-for-profit entities may provide information on letterhead from the Head of the Department confirming the organisation’s contact details and proof of right.

Documentation requirements for individual Applicants may include trustworthy, valid photo ID issued by a Government Agency (such as a passport).

QuoVadis may accept at its discretion other official documentation supporting an application. QuoVadis may also use the services of a third party to confirm Applicant information. QuoVadis accepts confirmation from third party organisations, other third party databases, and government entities.

Application Process

During the Certificate application process, QuoVadis [illegible]

Extended Validation SSL

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique number	
Issuer Signature Algorithm	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = QuoVadis Global SSL ICA OU = www.quovadisglobal.com O = QuoVadis Limited C = BM	
Validity Period	1 or 2 years expressed in UTC format	
Subject Distinguished Name		
Organization Name	subject:organisationName d<</M p-6(Q)0 Td (1)Tj 9)	This field MUST contain the Subject's full legal organisation name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organisation name in parenthesis. If the combination of the full legal organisation name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organisation name will be used.
Organisation Unit	subject:organisationUnit (2.5.6.5)	Information not verified.
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard Certificates are not allowed for EV Certificates.
City or Town of Incorporation	subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)	

Eligible Applicants

QuoVadis issues EV Certificates to Private Organizations, Government Entities, Business Entities and Non-Commercial Entities satisfying the requirements specified below:

(a) Private Organization Subjects

- The Private Organization MUST be a legally recognised entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation (e.g., by issuance of a Certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
- The Private Organization MUST have designated with the Incorporating Agency either a Registered Agent or Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;
- The Private Organization MUST NOT be designated on the records of the Incorporating Agency by labels such as "inactive," "invalid," "not current," or an equivalent facility;
- The Private Organization MUST have a verifiable physical existence and business presence.
- The Private Organization's Jurisdiction of Incorporation, Registration, Charter, or License and/or its Place of Business MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a Certificate by the laws of Bermuda; and
- The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda.

(b) Government Entity Subjects

- The legal existence of the Government Entity MUST be established by the political subdivision in which it operates;
- The Government Entity MUST NOT be in any country where QuoVadis is prohibited from doing business or issuing a Certificate by the laws of Bermuda; and
- The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Bermuda.

(c) Business Entity Subjects

Business Entities are entities that do not qualify as Private Organizations as defined in subsection (a) but do satisfy the following requirements. Business Entities may include general partnerships, unincorporated associations, sole proprietorships, and individuals (natural persons).

- The Business Entity MUST be a legally recognised entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, Certificate, or license, and whose existence can be verified with that Registration Agency;
- The Business Entity MUST have a verifiable physical existence and business presence;
- At least one Principal Individual associated with the Business Entity MUST be identified and validated;
- The identified Principal Individual MUST attest to the representations made in the Certificate Holder Agreement;
- Where the Business Entity represents itself under an assumed name, QuoVadis MUST verify the Business Entity's use of the assumed name;
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where QuoVadis is prohibited from doing business or issuing a Certificate under the laws of Bermuda; and
- The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be listed on any government denial list or prohibited list (such as a trade embargo) under the laws of Bermuda.

(d) Non-Commercial Entity Subjects

Non-Commercial Entities are entities who do not qualify under subsections (a), (b) or (c) above, but that do satisfy the following requirements:

- The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of International Organizations that have been approved for EV eligibility; and
- The International Organization Entity MUST NOT be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
- The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Subsidiary organizations or agencies of qualified International Organizations may also qualify for EV Certificates issued in accordance with the EV Guidelines.

- Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request. C /TT1 -460 Td - 0 13

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