PKI DISCLOSURE STATEMENT

Effective Date: 15 June 2017
Version: 1.1

Important Notice about this Document

This document is the PKI Disclosure Statement herein after referred to as the PDS. This document does not substitute or replace the Certificate Policy/Certification Practice Statement (CP/CPS) under which digital certificates issued by QuoVadis Limited (QuoVadis) are issued. You must read the CP/CPS at www.quovadisglobal.com/repository before you apply for or rely on a Certificate issued by QuoVadis.

The purpose of this document is to summarise the key points of the QuoVadis CP/CPS for the benefit of Subscribers, Certificate Holders and Relying Parties.

This document is not intended to create contractual relationships between QuoVadis and any other person. Any person seeking to rely on Certificates or participate within the QuoVadis PKI must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business. This version of the PDS has been approved for use by the QuoVadis Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA. The date on which this version of the PDS becomes effective is indicated on this document.

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement
QuoVadis PMA	15 June 2017	1.1	Based on ETSI TS319 411 model disclosure statement and eIDAS regulation

Table of Contents

1. CA CONTACT INFO

Bermuda and Group

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11,
Bermuda

Mailing Address:
QuoVadis Limited
Suite 1640
48 Par-La-Ville Road
Hamilton HM-11
Bermuda

Phone: +1-441-278-2800
Website: www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

Netherlands
QuoVadis Trustlink BV
Nevelgaarde 56 noord
3436 ZZ Nieuwegein
The Netherlands
Phone: +31 (0) 30 232-4320

Belgium
QuoVadis Trustlink BVBA
Schaliënhoevedreef 20T
2800 Mechelen
Belgium
Phone: +32 15 79 65 21

Germany
QuoVadis Trustlink Deutschland GmbH
Ismaninger Str. 52
D-81675 München
Telefon: +49-89-540-42-45-42

Switzerland
QuoVadis Trustlink Schweiz AG
Poststrasse 17
Postfach
9001 St. Gallen
Switzerland
Phone: +41-71-272-60-60

United Kingdom
QuoVadis Online Security Limited
Rhoades Mill, Main Road
Sibsey, Boston, Lincolnshire, PE22 0TW
United Kingdom
Phone: +44 (0) 333-666-2000

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate Profiles. The procedures for Digital Certificate Holder registration and validation are described below for each type of Digital Certificate issued. Additionally, specific Certificate Policies and QuoVadis' liability arrangements that are not described below or in the CP/CPS may be drawn up under contract for individual customers. Please refer to the CP/CPS for the full details.

Please note that where the term "Qualified Certificate" is used in this document it is consistent with the definition of "Qualified Certificate" in ETSI EN 319 411-2 and Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation").

2.1 QuoVadis Certificate Classes

QuoVadis Certificate Class	Description	QuoVadis / ETSI Certificate 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	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	Medium	Optional
QV Advanced +	Similar to the "QV Advanced" Certificate Class issued on a Secure Cryptographic Device. Based on the ETSI Normalised Certificate Policy requiring a secure cryptographic device (NCP+), which has the OID 0.4.0.2042.1.2	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.300 ETSI policy identifier OID: 0.4.0.2042.1.2	High	Yes
QV Qualified	QuoVadis Qualified Certificate on a Qualified Signature Creation Device (QSCD). Relevant to the Policy in ETSI EN 319 411-2 for: • EU qualified certificates issued to a natural person (QCP-n-qscd), with the policy identifier OID 0.4.0.194112.1.2. • EU qualified certificates issued to a legal person (QCP-l-qscd), with the policy identifier OID 0.4.0.194112.1.3.	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
	QuoVadis Qualified Certificate not on a Qualified Signature Creation Device (QSCD). Relevant to the Policy in ETSI EN 319 411-2 for: • EU qualified certificates issued to a natural person (QCP-n), with the policy identifier OID 0.4.0.194112.1.0. • EU qualified certificates issued to a legal person (QCP-l), with the policy identifier 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
QV Closed Community	Used for reliance by members of the Issuer community only. Policies are defined in the CP/CPS of the Issuing CA.	1.3.6.1.4.1.8024.1.500	Medium	Optional
QV Device	Issued to devices, including SSL Certificates. Includes Domain Controller certificates and Gateway certificates.	1.3.6.1.4.1.8024.1.600	Medium	Optional

2.2 Key Usage and Archive

Different QuoVadis Certificate Profiles may be issued with different key usages, and be eligible for key archive, according to the following table:

QuoVadis Certificate Type	Key Usage/ Extended Key Usage	Applicability of Certificate Types 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	Allowed (Archival only permitted for certain Issuing CAs. Not permitted for any CAs on European Trust Lists)	Allowed (Archival only permitted for certain Issuing CAs. Not permitted for any CAs on European Trust Lists)	Allowed (Archival not permitted)	Not Allowed
Signing	**Key Usage** digitalSignature nonRepudiation **Extended Key Usage** smartcardlogon clientAuth emailProtection	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)
Encryption	**Key Usage** keyEncipherment **Extended Key Usage** emailProtection	Allowed (Archival permitted)	Allowed (Archival permitted)	Allowed (Archival not permitted)	Not Allowed
Authentication	**Key Usage** digitalSignature **Extended Key Usage** smartcardlogon clientAuth	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Allowed (Archival not permitted)	Not Allowed

2.3 QV Standard

PURPOSE

Standard Digital 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 Digital 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 Certificate Holder.

2.4 QV Advanced

PURPOSE

QV Advanced Digital Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, encryption, and authentication.

REGISTRATION PROCESS

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

Unless the Certificate Holder has already been identified by the RA through a face-to-face identification meeting, accepted Know Your Customer (KYC) standards or a contractual relationship with the RA, validation requirements for a Certificate Holder shall include the following:

If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.
If the subject is a natural person evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the subject is a natural person who is identified in association with a legal person (e.g. the Subscriber), evidence of the identity shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

If the Certificate Holder is a natural person who is identified in association with a legal person (organisational entity), additional evidence shall be provided of:

- Full name and legal status of the associated legal person;
- Any relevant existing registration information (e.g. company registration) of the associated legal person; and
- Evidence that the Certificate Holder is affiliated with the legal person.

If the Certificate Holder is a legal person (organisational entity), evidence shall be provided of:

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

If the Certificate Holder is a device or system operated by or on behalf of a legal person, evidence shall be provided of:

- identifier of the device by which it may be referenced (e.g. Internet domain name);
- full name of the organisational entity;
- a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

2.5 QV Advanced +

PURPOSE

QuoVadis Advanced+ Digital Certificates are used for the same purposes as QuoVadis Advanced Digital 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).

Swiss Regulated Certificates issued under the Swiss Federal signature law (ZertES) are included in the QuoVadis Advanced+ certificate class. These certificates are issued out of the "QuoVadis Swiss Regulated CA G1" and have the notice text "regulated certificate" in the CertificatePolicies user notice. Swiss Regulated Certificates can be issued to natural and legal persons.

REGISTRATION PROCESS

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

The registration process and identity vetting process for QV Advanced + Certificates is the same as QV Advanced Certificates described in 2.3 above.

QuoVadis Advanced+ Digital Certificates must be issued on a Secure Cryptographic Device and adhere to the following requirements:

- Secure Cryptographic Device storage, preparation, and distribution is securely controlled by CA or RA;
- User activation data is securely prepared and distributed separately from the Secure Cryptographic Device;
- If keys are generated under the Certificate Holder's control, they are generated within the Secure Cryptographic Device used for signing or decrypting;
- The Certificate Holder's Private Key can be maintained under the subject's sole control; and
- Only use the Certificate Holder's Private Key for signing or decrypting with the Secure Cryptographic Device.

2.5.1 ElDI-V/GeBüV Certificates

The procedure below assumes an application by a company or organisation on behalf of its employees or devices for Digital Certificates.

PURPOSE

The ElDI-V/GeBüV Certificate is issued to organisations (companies, municipalities, etc.) and issued primarily to digitally sign electronic invoices. The Certificates may also be used for commercial purposes (such as legally-compliant electronic archiving according to GeBüV).

REGISTRATION PROCESS

These Digital Certificates are issued in accordance with ElDI-V (SR 641.201.1 and SR 641.201.1.1). Validation of these Certificates is performed in accordance with the validation procedures for QuoVadis Qualified Certificates and any additional validation requirements required by ElDI-V.

2.5.2 SuisseID Identity and Authentication Certificates

PURPOSE

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Identity and Authentication (IAC) Certificates help provide strong and secure authentication to applications.

Either a Common Name or a Pseudonym is required for a QuoVadis SuisseID IAC Certificate. Use of both Common Name and Pseudonym in the same Certificate is not permitted.

REGISTRATION PROCESS

QuoVadis SuisseID IAC Certificates are issued in accordance with the SuisseID requirements (including the "SuisseID Specification" document) using the QuoVadis SuisseID Signing Service. Unless stated otherwise in the SuisseID Specification document, the guidelines in TAV-ZERTES apply to the specification of QuoVadis SuisseID IAC Certificates.

For the issuance and life cycle management of SuisseID IAC Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant qualified certificate.

Evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Certificate Holder is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorization from an authorized Organisation representative; and
- Evidence that the Certificate Holder is associated with the organisational entity.

Private Keys for SuisseID IAC Certificates are generated and stored on a Hardware Security Module that meets FIPS PUB 140-2, level 3 or EAL 4 standards. This Hardware Security Module is located in a QuoVadis data centre. Access by the Certificate Holder to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone QSCD.

QuoVadis SuisseID IAC Certificates have a maximum validity of three years.

2.6 QV Qualified

2.6.1. eIDAS Qualified Certificate issued to a natural person on a QSCD

PURPOSE

The purpose of an EU Qualified certificates is to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation").

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key.

These certificates meet the relevant ETSI policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (QCP-n-qscd).

Swiss Qualified certificates issued under the Swiss Federal signature law (ZertES) also meet this ETSI policy QCP-n-qscd. These Swiss Qualified certificates are issued only to natural persons out of the "QuoVadis Swiss Regulated CA G1" and have the notice text "qualified certificate" in the CertificatePolicies user notice.

The content of these certificates meets the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

REGISTRATION PROCESS

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd). QuoVadis recommends that QCP-n-qcsd certificates are used only for electronic signatures.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:
i) by the physical presence of the natural person; or
ii) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Certificate Holder is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the Certificate Holder is associated with the organisational entity.

These Digital Certificates require a Qualified Signature Creation Device (QSCD) that meets the requirements laid down in annex II of Regulation (EU) N° 910/2014.

2.6.2 eIDAS Qualified Certificate issued to a natural person

PURPOSE

The purpose of these EU Qualified certificates are to identify the Certificate Holder with a high level of assurance, for the purpose of creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.

This type of QuoVadis Qualified certificates does not use a QSCD for the protection of the private key.

The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

REGISTRATION PROCESS

The identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for the "Policy for EU qualified certificate issued to a natural person" (QCP-n). The registration process for these certificates is the same as for the QCP-n-qcsd Certificates described in 2.5.1 above. The only difference is that these QCP-n certificates do not use a QSCD for the protection of the private key.

2.6.3 eIDAS Qualified Certificate issued to a legal person on a QSCD

PURPOSE

The purpose of these EU Qualified certificates are to identify the Certificate Holder with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person certificates an updated version of this CP/CPS will be published.

This type of QuoVadis Qualified certificates uses a QSCD for the protection of the private key.

These certificates meet the relevant ETSI policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (QCP-l-qscd). QuoVadis recommends that QCP-l-qscd certificates are used only for electronic seals.

The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

REGISTRATION PROCESS

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD" (QCP-l-qscd).

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:
i) by the physical presence by an authorized representative of the legal person; or
ii) using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which QuoVadis can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

Evidence shall be provided of:

- Full name of the organisational entity (private organisation, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices); and

- When applicable, the association between the legal person and the other organisational entity identified in association with this legal person that would appear in the organisation attribute of the certificate, consistent with the national or other applicable identification practices.

For the authorized representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

These Digital Certificates require a Qualified Signature Creation Device (QSCD) that meets the requirements laid down in annex II of Regulation (EU) N° 910/2014.

2.6.4. eIDAS Qualified Certificate issued to a legal person

PURPOSE

The purpose of these EU Qualified certificates are to identify the Certificate Holder with a high level of assurance, for the purpose of creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation.

QuoVadis will only begin issuing Qualified Legal Person certificates once the relevant audit has been passed and the service is listed on the relevant national Trust Services Lists. Once QuoVadis is permitted to issue Qualified Legal Person certificates an updated version of this CP/CPS will be published.

These certificates meet the relevant ETSI Policy for EU qualified certificate issued to a legal person (QCP-l). QuoVadis recommends that QCP-l certificates are used only for electronic seals.

The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

REGISTRATION PROCESS

Identity validation procedures for these Digital Certificates meet the relevant requirements of ETSI EN 319 411-2 for "Policy for EU qualified certificate issued to a legal person" (QCP-l).

The registration process for these certificates is the same as for the QCP-l-qcsd Certificates described in 2.5.3 above. The only difference is that these QCP-l certificates do not use a QSCD for the protection of the private key.

2.6.5 QV Qualified – SuisseID

PURPOSE

SuisseID is the first standardised electronic proof of identity in Switzerland (http://www.suisseid.ch/). QuoVadis SuisseID Qualified Certificates are used to sign documents electronically. The digital signature is tamperproof and legally equivalent to a handwritten signature.

Either a Common Name or a Pseudonym is required for QuoVadis SuisseID Qualified Certificate. Use of both Common Name and Pseudonym in the same Certificate is not permitted.

REGISTRATION PROCESS

QuoVadis SuisseID Qualified Certificates are issued in accordance with the SuisseID requirements (including the "SuisseID Specification" document) using the QuoVadis SuisseID Signing Service. Unless stated otherwise in the SuisseID Specification document, the guidelines in TAV-ZERTES apply to the specification of SuisseID Qualified Certificates.

For the issuance and life cycle management of SuisseID Qualified Certificates, QuoVadis adheres to the same organisational and operational procedures and uses the same technical infrastructure as for a ZertES compliant qualified certificate.

Evidence of the Certificate Holder's identity shall be checked against a physical person either directly, or shall have been checked indirectly using means which provide equivalent assurance to physical presence. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Certificate Holder is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity;
- Authorization from an authorized Organisation representative; and
- Evidence that the Certificate Holder is associated with the organisational entity.

Private Keys for SuisseID Qualified Certificates are generated and stored on a Hardware Security Module that meets FIPS PUB 140-2, level 3 or EAL 4 standards. This Hardware Security Module is located in a QuoVadis data centre. Access by the Certificate Holder to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a stand-alone SSCD.

QuoVadis SuisseID Qualified Certificates have a maximum validity of three years.

2.7 Closed Community Certificates

Closed Community Issuing CAs can, under contract, create Certificate Profiles to match the QuoVadis Standard Commercial Certificate for issuance to employees and affiliates.

Certificates issued by Closed Community Issuing CAs are for reliance by members of that community only, and as such a Closed Community Issuing CA can, by publication of a stand-alone certificate policy to its community issue various certificates that differ from the Standard Commercial Certificate.

QuoVadis must approve all closed community certificate policies to ensure that they do not conflict with the terms of the QuoVadis CP/CPS. Refer to the QuoVadis CP/CPS for further details of closed community certificates.

Under no circumstances can Closed Community Issuing CAs issue Qualified Certificates under European Digital Signature law.

2.8 QuoVadis Device

PURPOSE

QuoVadis Device Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. QuoVadis Device Certificates (i.e. with the OID 1.3.6.1.4.1.8024.1.600 in Certificate Policies) that have the Server Authentication Extended Key Usage comply with the CA/B Forum Baseline Requirements.

Device 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.

REGISTRATION PROCESS

QuoVadis acts as Registration Authority (RA) for Device Certificates it issues.

Before issuing a Device Certificate, QuoVadis performs procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorised to use the domain name and/or Organisation name to be included in the Certificate, and has accepted a Certificate Holder Agreement for the requested Certificate.

Documentation requirements for organisation Applicants may include, Certificate of Incorporation, Memorandum of Association, Articles of Incorporation or equivalent documents. 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.

Verification of Domain

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

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;

2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;

3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;

4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the FQDN;

5. Relying upon a Domain Authorization Document; and

6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the second-level domain for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the Fully Qualified Domain Name contains a 2 letter Country Code Top-Level Domain (ccTLD), then the domain level is whatever is allowed for registration according to the rules of that ccTLD.

Within 30 days after ICANN has approved a new gTLD for operation, QuoVadis (1) compares the new gTLD against the its records of valid certificates, (2) ceases issuing Certificates containing a Domain Name that includes the new gTLD until QuoVadis has first verified the Applicant's control over or exclusive right to use the Domain Name, and (3) revoke the Certificate within 120 days if the Applicant cannot demonstrate control over or exclusive right to use the Domain Name.

Where QuoVadis relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, QuoVadis verifies that the communication came from either the Domain Name Registrant (including any private,

anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. QuoVadis verifies that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by QuoVadis to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

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

2.9 SSL and Code Signing Certificates

QuoVadis issues three forms of Certificates according to the terms of the QuoVadis Root CA2 CP/CPS (www.quovadisglobal.com/repository):

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

ii. Extended Validation SSL Certificates are Certificates issued in compliance with the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) published by the CA/Browser Forum. The EV Guidelines are intended to provide enhanced assurance of identity of the Subscriber by enforcing uniform and detailed validation procedures across all EV-issuing CAs.

iii. Trusted Code Signing Certificates are Certificates issued in compliance with Code Signing Certificate Guidelines, including identification of the Certificate Holder by a verified organization name and certificate revocation for any misrepresentation or publication of malicious code.

3. RELIANCE LIMITS

Refer to section 9.8 of the CP/CPS (www.quovadisglobal.com/repository) for reliance limits. QuoVadis' liability for breach of its obligations pursuant to the QuoVadis CP/CPS shall, in the absence of fraud or wilful misconduct on the part of QuoVadis, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below:

Loss Limits/ Reliance Limits	Maximum per Certificate
Standard Certificates	US$250,000
Device Certificate	US$250,000
SuisseID Identity and Authentication (IAC) Certificates	CHF 10,000

In no event shall QuoVadis' liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular Digital Certificate to the intent that the loss limits reflect QuoVadis' total potential cumulative 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.

According to Digital Signature law (including ZertES, TAV SR 943.032.1 and ETSI EN 319 411-2 the only appropriate use for Qualified Digital Certificates is signing.

All events involved in the generation of the CA key pairs are recorded. This includes all configuration data and registration information used in the process. Audit logs are retained as archive records for a period no less than eleven (11) years for audit trail files, and no less than eleven (11) years for Key and Digital Certificate information.

4. OBLIGATIONS OF SUBSCRIBERS

Digital Certificate Holders are required to act in accordance with the CP/CPS and the relevant Certificate Holder/Subscriber Agreement. A Digital Certificate Holder represents, warrants and covenants with and to QuoVadis, Relying Parties, Application Software Vendors and the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing CA, Registration Authority, or QuoVadis immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorised viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorised use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key.
- Immediately notify the Issuing CA, Registration Authority or QuoVadis in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever. Following compromise, the use of the Certificate Holder's Private Key should be immediately and permanently discontinued.
- Take all reasonable measures to avoid the compromise of the security or integrity of the QuoVadis PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.
- Discontinue the use of the digital signature Key Pair in the event that QuoVadis notifies the Certificate Holder that the QuoVadis PKI has been compromised.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to be an Authorised Relying Party, a Party seeking to rely on a Digital Certificate issued within the QuoVadis PKI agrees to and accepts the Relying Party Agreement (www.quovadisglobal.com/repository) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

Authorised 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 Digital Certificate for any given purpose and that the use is not prohibited by the CP/CPS.
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.
- That the Digital Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

The Status of Digital Certificates issued within the QuoVadis PKI is published in a Certificate Revocation List (http://crl.quovadisglobal.com/<caname>.crl) or is made available via Online Certificate Status Protocol checking (http://ocsp.quovadisglobal.com) where available.

6. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

QuoVadis shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment (save as may arise directly from breach of the CP/CPS), wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

QuoVadis' liability to any person for damages arising under, out of or related in any way to the 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, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the QuoVadis PKI (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the QuoVadis PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to QuoVadis their acceptance of the foregoing and the fact that QuoVadis has relied upon the foregoing as a condition and inducement to permit that person to participate within the QuoVadis PKI.

Refer to the CP/CPS (www.quovadisglobal.com/repository) for further detail as to liability and warranties.

7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT CERTIFICATE POLICY

The following documents are available online at www.quovadisglobal.com/repository:

- Certificate Policy/Certification Practice Statements
- End User Certificate Holder Agreement
- SSL Certificate Subscriber Agreement
- Code Signing Certificate Subscriber Agreement
- Digital Certificate Terms and Conditions of Use
- Relying Party Agreement
- QuoVadis Time-Stamp Disclosure Statement
- QuoVadis Time-Stamp Policy/Practice Statement
- QuoVadis Time-Stamp Subscriber Agreement

8. PRIVACY POLICY

Data contained within a QuoVadis Certificate is considered public information. Personal data obtained during the registration process will not be released without prior consent of the relevant certificate holder, unless required otherwise by law or to fulfil the requirements of the CP/CPS. Refer to the QuoVadis Privacy Statement at http://www.quovadisglobal.com/privacy.aspx.

9. REFUND POLICY

QuoVadis or Issuing CAs under the QuoVadis hierarchy may establish a refund policy, details of which may be contained in relevant contractual agreements. Refer to section 9.1.5 of the CP/CPS (www.quovadisglobal.com/repository).

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1 Governing Law

Subscribers and Relying Parties shall use QuoVadis Certificates and any other related information and materials provided by QuoVadis only in compliance with all applicable laws and regulations. QuoVadis may refuse to issue or may revoke Certificates if, in the reasonable opinion of QuoVadis, issuance or the continued use of the QuoVadis Certificates would violate applicable laws or regulations.

QuoVadis Certificates issued by QuoVadis are governed by the laws of the country referred to in the Subscriber Agreement for the Certificate in question, without reference to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods.

10.2 Dispute Resolution

Any controversy or claim between two or more participants in the QuoVadis PKI (for these purposes, QuoVadis shall be deemed a "participant" within the QuoVadis PKI) arising out of or relating to the QuoVadis CP/CPS shall be shall be referred to an arbitration tribunal.

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

- Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.
- Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.
- Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

For Qualified Certificates issued in accordance with Swiss Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in Switzerland.
For Qualified Certificates issued in accordance with Dutch Digital Signature law, such arbitration shall, unless agreed otherwise between the parties take place in The Netherlands.
For Qualified Certificates, in accordance with the Belgian Digital Signature law, all disputes shall be dealt with under Belgian Law.
For Qualified Certificates issued in other jurisdictions, disputes will be dealt with under the national law of the relevant Member State.

11. CA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

Refer to https://www.quovadisglobal.com/AboutUs/Accreditations.aspx for a list of QuoVadis' audits and accreditations.