digicert® + QuoVadis

QuoVadis
PKI Disclosure Statement

OIDs:	1.3.6.1.4.1.8024.0.1 1.3.6.1.4.1.8024.0.2 1.3.6.1.4.1.8024.0.3
Effective Date:	June 5, 2019

Important Notice

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 (also provides a mechanism for submission of revocation requests)
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").
In the case of Qualified certificates, where QuoVadis manages the keys on behalf of the Certificate Holder, QuoVadis shall require:

- where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures are only created by the QSCD;

- in the case of natural persons, the Certificate Holders' private key is maintained and used under their sole control and used only for electronic signatures; and
- in the case of legal persons, the private key is maintained and used under their control and used only for electronic seals.

2.1 QuoVadis Certificate Classes

QuoVadis Certificate Class	Description	QuoVadis / ETSI Certificate Policy OID	4006.72 6)1.3n(15. 6n134/A

2.2

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.

2.5.2 SuisseID Identity and Authentication Certificates

PURPOSE

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.

2.6.2 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

5: C (5 10.T([(5:)2 j0.004 Tc -0011 Tw 9 6 (lEMC 0 Tw (-)Tref548.76 698.g(and c 4711/Art548.76 (

2.6.5 QV Qualified

9. 4124;and

4. OBLIGATIONS OF CERTIFICATE HOLDERS

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 pa0.7 (()3.7 5atfed tk13.3 (nci)-0.7 (n(ut)2 (o)13.3 (t)3 (p)13.3 ( )13.7 (a)13.3 (u)13.4 (t)2 (v)-0

10.2 Dispute Resolution

Complaints can be communicated to QuoVadis via the QuoVadis website using the “Contact Us” link at https://www.quovadisglobal.com/ContactUs.aspx.