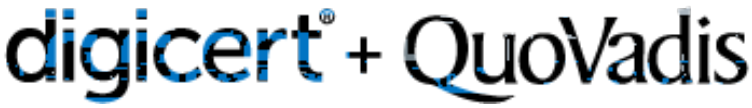
PKI Disclosure Statement



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 20, 2019
Version:	1.7

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. This PKI Disclosure Statement relates to the following CP/CPS documents:

- CP/CPS for Root CA and Root CA3
- CP/CPS for Root CA2

You must read the relevant 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.

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
QuoVadis PMA	13 September 2017	1.2	Updates for submission of complaints.
QuoVadis PMA	20 August 2018	1.3	Updates for Qualified Website Authentication Certificates and link to Privacy Notice.
QuoVadis PMA	30 august 2018	1.4	Update for Qualified website authentication certificates information
QuoVadis PMA	7 December 2018	1.5	Updates to include changes for EU Qualified certs and itsme Sign Issuing CA G1. More explicit reference to the BR Domain Vetting methods.
QuoVadis PMA	5 June 2019	1.6	Updates for where QSCD managed on behalf of Certificate Holder by QuoVadis.
QuoVadis PMA	20 June 2019	1.7	Updates for PSD2 QCP-w-psd2 and QSealC.

- 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

	x EU qualified certificates issued to a natural person (QCP-n-qscd), with the policy identifier OID 0.4.0.194112.1.2 x EU qualified certificates issued to a legal person (QCP-l-qscd), with the policy identifier OID 0.4.0.194112.1.3	(QCP-l-qscd)		
	QuoVadis Qualified Certificate not on a Qualified Signature Creation Device (QSCD). Relevant to the Policy in ETSI EN 319 411-2 for: x EU qualified certificates issued to a natural person (QCP-n), with the policy identifier OID 0.4.0.194112.1.0. x EU qualified certificates issued to a legal person (QCP-l), with the policy identifier OID 0.4.0.194112.1.1. x May include PSD2 fields	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.450 ETSI policy identifier OIDs: x 0.4.0.194112.1.0 (QCP-n) x 0.4.0.194112.1.1 (QCP-l)	High	No
	QuoVadis qualified website authentication certificate (QCP-W) Relevant to the policy in ETSI EN 319 411-2 for: x EU qualified certificates issued to a website (QCP-w), with the policy identifier OID 0.4.0.194112.1.4 PSD2 QWAC (QCP-P61)l)Q 0 Tc 0TJ -0.0CP13.72 0(ad)]TJ [(c)-5..6 94(IDs)-2..001 T6>>BDC82t0 T(.)1.283			

2.4. QV ADVANCED

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.

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

Unless the Certiq9(83.4.8 (1ql)-78(of)0.8 (th)-4.8 ((r)3.3)-11.92)-16.8 (a)8 (e)5 (d)-11.9 (r)3.-3 (9-11.(e)5 <</MCI3.4.8 11

2.5. QV ADVANCED +

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.

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

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 Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

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

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.

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.

on behalf of the Certificate Holder and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 1.3.6.1.4.1.8024.1.410 OID in certificate policies.

- For PSD2 Certificates, additional steps verify specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA.

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 ele3 (e)5.1 (o)-W-5.8 (y)-3 (f)-11.3 (or)3. s andtha (y)-3(th)-

QuoVadis Qualified Website Authentication (QCP-

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.

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. Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation)
2. Communicating directly with the Domain Name Registrant by calling their phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The phone number used must be the number listed by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.3;
3.

2.

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

- 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.

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 (https://www.quovadisglobal.com/repository) for further detail as to liability and warranties.

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

- Certificate Policy/Certification Practice Statements
- Certificate Holder 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

In the context of the itsme Issuing CA G1 the Certificate Holder Agreement is referred to as the Terms and Conditions.

Refer to the Privacy Notice for Digital Certificates and Signing Solutions at: https://www.quovadisglobal.com/privacy_statement/.

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 (https://www.quovadisglobal.com/repository).

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

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