DigiCert Europe PKI Disclosure Statement

Version 2.01, 16 January 2025

Contents

This document is the PKI Disclosure Statement (PDS) of DigiCert Europe (formerly known as QuoVadis), a company of DigiCert, Inc. The purpose of this document is to summarise the key points of the DigiCert Europe CP/CPS for the bene f t of Subscribers and Relying Parties.

This document does not substitute or replace the Certi f cate Policy/Certi f cation Practice Statement (C £

Customer complaints email: qvcomplaints@digicert.com

- Bermuda: DigiCert Bermuda Limited (previously QuoVadis Limited), Washington Mall 3F, 7 Reid Street, Hamilton HM-11, Bermuda. Phone: +1-441-278-2800
- Belgium: DigiCert Europe Belgium BV (previously QuoVadis Trustlink BVBA), Schaliënhoevedreef 20T, 2800 Mechelen, Belgium. Phone: +32 15-79-65-21
- Germany: DigiCert Deutschland GmbH (previously QuoVadis Trustlink Deutschland GmbH), Ismaninger Str. 52, D-81675 München, Germany. Phone: +49-89-540-42-45-42
- Ireland: DigiCert Ireland Limited, 3 Dublin Landings, North Wall Quay, Dublin 1, D01C4EO, Ireland. Phone +353 1803 5400.
- Netherlands: DigiCert Europe Netherlands BV (previously QuoVadis Trustlink Netherlands BV), Nevelgaarde 56 noord, 3436 ZZ Nieuwegein, The Netherlands. Phone: +31 (0) 30 232-4320
- Switzerland: DigiCert Switzerland AG (previously QuoVadis Trustlink Schweiz AG), Poststrasse 17, Postfach, 9001 St. Gallen, Switzerland. Phone: +41 71-228-98-00
- United Kingdom: QuoVadis Online Limited, 2 Harbour Exchange Square, London, E14 9GE, United Kingdom. Phone: +44 (0) 333-666-2000

DigiCert Europe provides additional information for entities requiring assistance with revocation or an investigative report at https://www.quovadisglobal.com/certificate-revocation. See also Section 4.9.2 of the CP/CPS.

For anyone listed in Section 4.9.2 of the relevant CP/CPS and the CA/Browser Baseline Requirements that requires assistance with revocation or investigative reports, DigiCert Europe provides this page for reporting and submitting requests with all of the necessary information as outlined in Section 4.9: https://problemreport.digicert.com/

If the problem reporting page is unavailable, there is a system outage, or you believe our findings are incorrect please contact revoke@digicert.com. During office hours (CET), problem reports and revocation requests can also be made using the DigiCert Europe RA and support line +31 (0) 30 232 4320. Outside of office hours CET the emergency revocation hotline can be used at +1 651 229 3456. Typically, the following information is required:

- Common Name
- Certificate serial number
- E-mail address of the Subje † Б У y,

	OID 0.4.0.194112.1.2 EU Qualified Certificates issued to a legal person (QCP-l-qscd), with the OID 0.4.0.194112.1.3	0.4.0.194112.1.3 (QCP-l-qscd)		
	Qualified Certificate not on a QSCD.+ Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCPl), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.450 ETSI policy identifer OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
	Qualified Certificate not on a QSCD, where the device is managed by a QTSP. Relevant to the Policy in ETSI EN 319 411-2 for: EU Qualified Certificates issued to a natural person (QCP-n), with the OID 0.4.0.194112.1.0 EU Qualified Certificates issued to a legal person (QCPl), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.460 ETSI policy identifer OIDs: 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.1 (QCP-l)	High	No
Closed Community	Used for reliance by members of the Issuer community only. Policies	1.3.6.1.4.1.8024.1.500	Medium	Optional

following identity proofing methods and the related terms and conditions. DigiCert Europe may provide alternative identity verification methods available to the relevant Certificate Class:

- Physical presence;
- Remote Identity Verification which provides equivalent assurance in terms of reliability to the physical presence;
- Reliance on an Electronic Signature; and/or
- Video verification.

The Subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the Subject's sole control.

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

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

These Certificates meet the relevant ETSI "Policy for EU qualified ce ɗ ɥ the PSD È ali f

ETSI EN 319 411-2 defnes “QCP-w” as the “policy for EU Quali fed website certi fcate issued to a natural or a legal person and linking the website to that person”. DigiCert Europe policy is that DigiCert Europe Quali fed Website Authentication (QCP-w) Certi fcates will only be issued to legal persons and not natural persons.

DigiCert Europe QCP-w Certi fcates will be issued under the requirements of ETSI EN 319 411-2 aim to support website authentication based on a Quali fed defned in articles 3 (38) and 45 of the eIDAS Regulation.

QCP-w Certi fcates issued under these requirements endorse the requirement of EV Certi fcates whose purpose is speci fed in clause 5.5 of ETSI EN 319 411-1 [2]. In addition, EU Quali fed Certi fcates issued

Subjects may include an Individual (natural person) or a natural person identified in association with an

and/or Organisation name to be included in the Certificate, and has accepted a Subscriber 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). DigiCert Europe may accept at its discretion other official documentation supporting an application. DigiCert Europe may also use the services of a third party to confirm Applicant information.

1. Business SSL Certificates are Certificates for which limited authentication and authorisation checks are performed on the Subscriber and the individuals acting for the Subscriber (OID 1.3.6.1.4.1.8024.0.2.100.1.1).
2. Extended Validation SSL Certificates are issued in compliance with the "Guidelines for the Issuance and Management of Extended Validation Certificates" published by the CA/Browser Forum (OID 1.3.6.1.4.1.8024.0.2.100.1.2).
3. Qualified Website Authentication Certificates (QWAC) are Certificates issued in compliance with the eIDAS Regulation (OID 0.4.0.194112.1.4) or for PSD2 (also with OID 0.4.0.19495.3.1). See also Section 2.6.6.

DigiCert Europe confirms that the Applicant either is the Domain Name Registrant or has control over the FQDN by methods described in Section 3.2.2.4 of the CA/Browser Forum Baseline Requirements.

DigiCert Europe verifies an Applicant's or Organisation's right to use or control of an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following:

- By verifying domain control

Any appropriately authorised party may request revocation of a Certificate. This may include a recognised representative of a Subscriber or the RA, the party that purchased the Certificate on behalf of a Subscriber, and the party that manages the Portal account to which the Certificate is tied. DigiCert Europe may revoke a Certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity

Subscribers represent to DigiCert Europe, Application Software Suppliers, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise, and exercise sole and complete control and use of its Private Keys;
2. Provide accurate and complete information when communicating with DigiCert Europe, and to respond to DigiCert Europe's instructions concerning Key Compromise or Certificate misuse;
3. Confirm the accuracy of the certificate data prior to installing or using the Certificate;
4. For Qualified Certificates: (a) If the policy requires the use of a QSCD, Electronic Signatures must only be created by a QSCD, (b) In the case of natural persons, the Private Key should only be used for Electronic Signatures, and (c) In the case of legal persons, the Private Key must be maintained and used under the control of the Subscriber and it should only be used for Electronic Seals.
5. Promptly request revocation of a Certificate, cease using it and its associated Private Key, and notify DigiCert Europe if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. For Remote Identity Verification, use the identity proofing software distributed by DigiCert Europe. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;
7. Ensure that individuals using Certificates on behalf of an organisation have received security training appropriate to the Certificate;
8. Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, the CP/CPS, and the relevant Subscriber Agreement, including only installing TLS/SSL Server Certificates on servers accessible at the Domain listed in the Certificate and not using code signing Certificates to e riber v '

- To be relied upon as an EU Qualified Certificate, the CA/trust anchor for the validation of the Certificate shall be as identified in a service digital identifier of an EU Trusted List entry with service type identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC" for a QTSP.
- ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted

In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that: (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Customer is Domiciled in or the Services are:	Governing Law is:	Court or arbitration body with exclusive jurisdiction:
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah
Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in the below city corresponding to the DigiCert Europe