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:	December6, 2021
Version:	1.13

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 May 2008	1.0	Based on ETSI TS101 456 model disclosure statement

[redacted]

TABLE OF CONTENTS

1. CA CONTACT INFO

Website:

2. CERTIFICATE TYPE, VALIDATION, PROCEDURES AND USAGE

Within the QuoVadis PKI an Issuing CA can only issue Certificates with approved Certificate Profiles. The procedures for Subscriber registration and validation are described below for each type of 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"). QuoVadis Qualified CAs are listed on the EU Trusted List (EUTL) for the Netherlands and for Belgium.

In the case of Qualified Certificates, where QuoVadis manages the keys on behalf of the Subscriber, QuoVadis shall require:

- where the policy requires the use of a Qualified SignatunQuBation Device (QSnD) then the signatuuBs are only cQuBated by the QSCD;
- in the case of natuQual peQusons, the Subscriber

Certificate Class	Description	Policy OID	Assurance Level	Requires token?

Certificate Class	Description	Policy OID	Assurance Level	Requires token?
	QuoVadis 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 (QCP-l), with the OID 0.4.0.194112.1.1	QuoVadis Certificate Class OID: 1.3.6.1.4.1.8024.1.460 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 Time-stamp Certificates	1.3.6.1.4.1.8024.1.600	Medium	Optional

QuoVadis provides test certificates for all types of Certificates.

2.2. KEY USAGE AND ARCHIVE

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

QuoVadis Certificate Type	Key Usage/ Extended Key Usage Options	Applicability to QuoVadis Certificate Classes			
		QV Standard	QV Advanced	QV Advanced +	QV Qualified
Signing and Encryption	Key Usage digitalSignature				

2.3. IDENTITY AUTHENTICATION

If the Subjectis an Organisation(legal person), evidence shall be provided of:

i) Full name of the legal person;

2.4. CERTIFICATE CLASSES

2.4.1. QV Standard

Purpose

Standard Certificates provide flexibility for a range of uses appropriate to their reliance value including S/MIME, electronic signatures, authentication, and encryption.

May use RIV4 for NFC with RIV2 as a fallback option if NFC is not available. Storage of personal data is in accordance with ZertES.

Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS 140-2 level 3 or EAL 4 standards. This Hardware is either a USB-token handed out to clients or a HSM located in a QuoVadis datacentre. The level of assurance using a HSM aims to be the same as achieved by a stand-alone SSCD. Access by the Subscriber to the keys is protected using multifactor authentication.

Swiss Regulated Certificates have a maximum validity of three years.

2.4.3.2. *Swiss Regulated Certificate issued to a Legal Person (Company Seal)*

Purpose

Swiss Regulated Certificates (non qualified) issued under the Swiss Federal signature law (ZertES) are included in the QV Advanced+ Certificate Class. Swiss Regulated Certificates are issued out of the “QuoVadis Swiss Regulated CA” and have the notice text “regulated certificate” in the CertificatePolicies user notice.

Registration Process

Swiss Regulated Certificates are issued in accordance with the ZertES requirements using the QuoVad Signing Service. The guidelines in TAV-ZERTES apply to the specification of Swiss Regulated Certificates.

Subjects may include an Organisation (legal person). Only methods approved for ZertES may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Identity proofing may be conducted via physical presence, remote identity verification, reliance on electronic signature, or video identification. May use RIV4 for NFC with RIV2 as a fallback option if NFC is not available. Storage of personal data is in accordance with ZertES.

Private Keys for Swiss Regulated Certificates are generated and stored on a Hardware that meets FIPS 140-2 level 3 or EAL 4 standards. This Hardware is either a USB-token handed out to clients or an HSM located in a QuoVadis datacentre. The level of assurance using an HSM aims to be the same as achieved by a stand-alone SSCD. Access by the Subscriber to the keys is protected using multifactor authentication.

Swiss Regulated Certificates have a maximum validity of three years.

2.4.4. QV Qualified

2.4.4.1. *eIDAS Qualified Certificate issued to a Natural Person on a QSCD*

Purpose

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

- ETSIEN 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

Identity validation procedures for these Certificates meet the relevant requirements of ETSI EN 319 411-2 for “Policy for EU qualified certificate issued to a natural person where the

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.

2.4.4.3. *eIDAS Qualified Certificate issued to a Legal Person on a QSCD*

Purpose

The purpose of these EU Qualified Certificates are to identify the Subscriber with a high level of assurance, for the purpose of creating Qualified Electronic Seals meeting the qualification cea41.9 (th)-3.3 (ath)-3.sa-0.0

2.4.4.4. *eIDAS Qualified Certificate issued to a Legal Person*

Purpose
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 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 • ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
Registration Process
Identity validation procedures for these 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-qscd Certificates. The only difference is that these QCP-l certificates do not use a QSCD for the protection of the private key. Subjects may include an Organisation (legal person). Only methods approved for eIDAS Qualified Certificates may be used to verify the identity, authorisation, and approval of the authorised representative of the legal person. *See* Section 3.2.2 and 3.2.3. Identity proofing may be conducted via physical presence, remote identity verification (RIV4 only), or reliance on eID or electronic signature. 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 recognized identifier, and PSD2 roles. These details are provided by the Certificate Applicant and confirmed by QuoVadis using authentic information from the NCA.

2.4.4.5. *Swiss Qualified Certificate*

Purpose
QV Swiss Qualified Certificates are Qualified personal certificates according to the Swiss Federal signature law (ZertES). They are issued out of the “QuoVadis Swiss Regulated CAs” and have the notice text “qualified certificate” in the Certificate Siifar Fa3-4.7 (s)-4 (r)3.4 (tif) 8 (a)-7o.2 (s)-4ti.1 (d)6..8 (e)-7 (r)3.J 0 Tc 0 Tw 5.98(u

Subjects may include an Individual (natural person) or a natural person identified in association with an Organisation. *See* Section 3.2.2 and 3.2.3 of the relevant CP/CPS. Only remote identity verification means approved according to ZertES may be used. Identity proofing may be conducted via physical presence; remote identity verification, or reliance on electronic signature. May use RIV4 for NFC with RIV2 as a fallback option if NFC is not available. Only a valid passport or national ID is accepted as evidence. Storage of personal data is in accordance with ZertES.

Private Keys for QVSwissQualified Certificates are generated and stored on an HSM Hardware Security Module or USB token that meets the ZertES requirements, FIPS 140-2, level 3 or EAL 4 standards. HSMs for QuoVadis Signing Services are located in QuoVadis datacentres. Access by the Subscriber 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.

QVSwissQualified Certificates have a maximum validity of three years; in special use-cases they are issued with a validity of only one hour.

uieaielt(u)-4.7D .3 (.)401fh.9(ielt 00b3 (seq)P10.9(ieli)) -000b3 (sem)2 3 k6.9((0 Tw 16)2 2u)-37353.2 f853400106 TdT9(a52332

2.4.5. 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.

2.4.6. QuoVadis Device Certificates

Purpose
QuoVadis Device Certificates are intended for a variety of uses including for Time-stamp Authority (TSA) applications (1.3.6.1.4.1.8024.1.600). QuoVadis Device Certificates that have the serverAuth Extended Key Usage comply with the CA/B Forum Baseline Requirements.
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 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). 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.

2.4.7. TLS/SSL Certificates

i) 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)

ii) 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).

iii) 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.

Validation of Domain and Email Authorisation and Control
For each FQDN listed in a TLS Certificate, QuoVadis 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.

QuoVadis 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 over the email Domain Name using one of the procedures listed in this section; or
- by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response within a limited period of time that includes the Random Value to indicate that the Applicant controls that same email address.

Authentication For An IP Address
For each IP Address listed in a Certificate, QuoVadis confirms that the Applicant controlled the IP Address by methods described in Section 3.2.2.5 of the CA/Browser Forum Baseline Requirements.

2.4.8. Code Signing Certificates

Code Signing Certificates are Certificates issued in compliance with the Minimum Requirements for the

CERTIFICATE WILL MEET SUBSCRIBER’S OR ANY OTHER PARTY’S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

QuoVadis does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time. Subscriber’s sole remedy for a defect in the Certificates is for QuoVadis to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that QuoVadis has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Certificates or combination of the Certificates with other products and services by parties other than QuoVadis, or (ii) Subscriber’s breach of any provision of the Subscriber Agreement

7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT CERTIFICATE POLICY

The QuoVadis Master Services Agreement references and makes the Certificate Terms of Use, Privacy Policy and relevant QuoVadis CP/CPS part of the Terms and Conditions. The itsme Issuing CA provides its own Terms and Conditions. The relevant documents are available online at https://www.quovadisglobal.com/repository .

8. PRIVACY POLICY

QuoVadis follows the Privacy Notices posted on its website when handling personal information. *See* https://www.quovadisglobal.com/privacy-policy. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1)

Customer is Domiciled in:	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

not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding (“Class Action”). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to