TIME-STAMPING AUTHORITY (TSA) DISCLOSURE STATEMENT

Effective Date: 25 November 2016
Version: 1.5

Important Notice about this Document

This document is the Time-Stamping Authority (TSA) Disclosure Statement herein after referred to as the TSA Disclosure Statement. This document does not substitute or replace the QuoVadis Time-Stamp Policy/Practice Statement (QV-TSP/PS) or the QuoVadis Certificate Policy/Certification Practice Statement (CP/CPS). You must read the QV-TSP/PS and the CP/CPS at http://www.quovadisglobal.com/repository before you apply for the QuoVadis Time-Stamping Service.

The purpose of this document is to provide a set of statements about the policies and procedures of the TSA that require particular emphasis or disclosure to subscribers and relying parties. This document is not intended to create contractual relationships between QuoVadis Limited ("QuoVadis" or "QV") 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 TSA Disclosure Statement 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 TSA Disclosure Statement becomes effective is indicated on this document.

Version Control

Author	Date	Version	Comment
QuoVadis PMA	21 March 2006	1.0	Initial Draft based on ETSI TS102 023 model TSA disclosure statement
QuoVadis PMA	23 June 2008	1.1	Updates to URLs and updates based on ETSI TS102 023 model TSA disclosure statement
QuoVadis PMA	29 June 2010	1.2	Updates to algorithms
QuoVadis PMA	11 October 2010	1.3	Updates to include more detail on validity period of TSA certificate
QuoVadis PMA	25 May 2012	1.4	Updates for trusted time source and supported algorithms
QuoVadis PMA	24 November 2016	1.5	Updates for eIDAS, Regulation (EU) No 910/2014. Updates for ETSI EN 319 421 and ETSI EN 319 422.

Table of Contents

1. ENTIRE AGREEMENT

This TSA Disclosure Statement provides high level disclosures regarding the QuoVadis Time-stamp Authority (QV-TSA). It does not replace or override the definitive QuoVadis policy and practice documents which are available at http://www.quovadisglobal.com/repository.

2. TSA CONTACT INFO

The QV-TSA is operated by QuoVadis Limited.

Bermuda and Group

Corporate Offices:	*Mailing Address:*
QuoVadis Limited	QuoVadis Limited
3rd Floor Washington Mall	Suite 1640
7 Reid Street,	48 Par-La-Ville Road
Hamilton HM-11,	Hamilton HM-11
Bermuda	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) 30 232-43-20

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

Belgium
QuoVadis Trustlink BVBA
Schaliënhoevedreef 20T
2800 Mechelen
Belgium
Phone: +32 (0) 15 79 65 21

Germany
QuoVadis Trustlink Deutschland GmbH
Feringastraße 10b
D-85774 Unterföhring / München
Germany
Phone: +49-89-540-42-45-42

3.   TIME-STAMP TOKEN TYPES AND USAGE

The QV-TSA aims to deliver time-stamping services in accordance with the Regulation (EU) No 910/2014 ("eIDAS Regulation"). However, QuoVadis time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time. Supported signing algorithms are sha256WithRSAEncryption (2048 bit key length).

Acceptable Time Stamp Request Hashes include SHA-256, SHA-384 and SHA-512. The QuoVadis digital signature on the Time-Stamp Token (TST) has a validity period of up to ten years. Refer to section 6 below for information on how to verify a TST. Use of the QuoVadis TSA may be limited to Certificate Holders of a valid QuoVadis digital certificate. QuoVadis may charge fees for the services provided by the QuoVadis TSA.

The object-identifier (OID) of the QuoVadis Time-Stamping Policy is: 1.3.6.1.4.1.8024.0.2000.6. This OID is referenced in every QuoVadis-issued time-stamp and also the QV-TSP/PS. This QuoVadis Time-Stamping Policy is based on the ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1).

The QV-TSA has responsibility for the operation of one or more Time-Stamping Units (TSU) which create and sign TSTs on behalf of the TSA. Each TSU has a different key. Refer to the "QuoVadis TSAs" section of the following QuoVadis web page for a list of QuoVadis TSUs:
https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx.

Below is a summary of the current QuoVadis TSUs and their issuers:

QuoVadis TSU Subject Distinguished Name	TSU Issuer	National Trust List relating to TSU Issuer
CN = eutsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.7 OU = Time-stamp Authority O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	QuoVadis EU Issuing Certification Authority G4	The Netherlands (https://www.acm.nl/en/tsl/)
CN = eutsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.7 OU = Time-stamp Authority O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	QuoVadis EU Issuing Certification Authority G4	The Netherlands (https://www.acm.nl/en/tsl/)
CN = betsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.6 OU = Time-stamp Authority O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	QuoVadis Belgium Issuing CA G2	Belgium (https://tsl.belgium.be/)
CN = betsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.6 OU = Time-stamp Authority O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	QuoVadis Belgium Issuing CA G2	Belgium (https://tsl.belgium.be/)
CN = tsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.3 OU = Thales TSS ESN:B87E-D107-917F OU = Time-stamp Authority O = QuoVadis Limited C = CH	QuoVadis Root Certification Authority	N/A – Issued by a QuoVadis Root CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.

QuoVadis TSU Subject Distinguished Name	TSU Issuer	National Trust List relating to TSU Issuer
CN = tsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.0 OU = nCipher DSE ESN:FBC9-3056-CE0A OU = Time-stamp Authority O = QuoVadis Limited C = CH	QuoVadis Root Certification Authority	N/A – Issued by a QuoVadis Root CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.

4.   RELIANCE LIMITS

QuoVadis does not set reliance limits for timestamp services, however reliance limits may be set by applicable law or by agreement. See Limitation of Liability below. The QV-TSA assures time with ±1 second of a trusted UTC time source. If a trusted UTC time source cannot be acquired the time stamp will not be issued. QuoVadis maintains secure records concerning the operation of the QV-TSA for a period of 11 years for the purpose of providing evidence in legal proceedings.

5.   OBLIGATIONS OF SUBSCRIBERS

Subscribers must verify that the time-stamp token has been correctly signed and check the QuoVadis CRL to confirm that the private key used to sign the time-stamp token has not been compromised. Subscribers must use secure cryptographic functions for time-stamping requests a method or software toolkit approved by QuoVadis to create time-stamps, unless otherwise specifically authorised in writing by QuoVadis. Subscribers must inform its end users (including any relevant Relying Parties) about the QV-TSP/PS, the CP/CPS.

6.   TIME-STAMPING UNIT (TSU) PUBLIC KEY STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Before placing any reliance on a Time-Stamp, relying parties must verify that the TST has been correctly signed and that the associated TSU certificate has not been revoked. QuoVadis CA Certificates, TSU Certificates and the related CRLS are published at https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx.   If this verification takes place after the end of the validity period of the certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

The Relying Party should take into account any limitations on usage of the time-stamp indicated by this QV-TSP/PS, the Time-Stamping Authority Subscriber Agreement and any other precautions documented by QuoVadis.

Note that QuoVadis has a number of different TSU Certificates, signed by different QuoVadis Issuing CAs. It is important that Relying Parties refer to https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx to determine the relevant TSU as this may also impact reliance.

ETSI EN 319 421 contains some additional requirements for Qualified electronic time-stamps as per Regulation (EU) No 910/2014. ETSI EN 319 421 states:

> "The relying party is expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified."

QuoVadis are currently operating under the transitional measures (Article 51) of the eIDAS Regulation. The public keys of the QuoVadis TSUs are not currently listed on any Trusted List. The issuers of some QuoVadis TSUs are listed on Trusted Lists. A summary of the QuoVadis TSUs, issuers and Trusted Lists is provided in section 3 above.

7.   RETENTION OF EVENT LOGS

TSA event logs are retained for 11 years in accordance with the retention period for audit logs in the CP/CPS.

8.   LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

QuoVadis undertakes to operate the QV-TSA in accordance with the QV-TSP/PS, the CP/CPS, and the terms of agreements with the Subscriber. QuoVadis makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

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 QV-TSP/PS or 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 bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified digital certificates relied upon in accordance with specific national laws and regulations. These liabilities are described in section 9.8 (Liability and Limitations of Liability) of the CP/CPS.

9. APPLICABLE AGREEMENTS AND PRACTICE STATEMENT
See the QV-TSP/PS and the QuoVadis CP/CPS at http://www.quovadisglobal.com/repository.

10. PRIVACY POLICY
The QV-TSA complies with applicable legal requirements, as well as the requirements of the European Data Protection Directive [Dir 95/46/EC]. QV-TSA records shall be completely protected from disclosure unless with Subscriber agreement or by court order or other legal requirement.

11. REFUND POLICY
QuoVadis does not refund fees for time-stamp services.

12. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION
The QV-TSA aims to deliver time-stamping services used in support of qualified electronic signatures (i.e., in line with the eIDAS Regulation), as well as under other applicable laws and regulations.

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

13. TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT
Refer to https://www.quovadisglobal.com/AboutUs/Accreditations.aspx for a list of QuoVadis' audits and accreditations.