



## **TIME-STAMPING AUTHORITY (TSA) DISCLOSURE STATEMENT**

**Effective Date: 29 June 2010**

**Version: 1.2**

Copyright © QuoVadis 2010. All rights reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by QuoVadis.

### 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

### Table of Contents

- 1. ENTIRE AGREEMENT ..... 1
- 2. TSA CONTACT INFO ..... 1
- 3. TIME-STAMP TOKEN TYPES AND USAGE..... 1
- 4. RELIANCE LIMITS ..... 1
- 5. OBLIGATIONS OF SUBSCRIBERS ..... 2
- 6. TIME-STAMPING UNIT (TSU) PUBLIC KEY STATUS CHECKING OBLIGATIONS OF RELYING PARTIES ..... 2
- 7. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY ..... 2
- 8. APPLICABLE AGREEMENTS AND PRACTICE STATEMENT ..... 2
- 9. PRIVACY POLICY ..... 2
- 10. REFUND POLICY..... 2
- 11. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION ..... 2
- 12. TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT ..... 3

**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:*

QuoVadis Limited  
3rd Floor Washington Mall  
7 Reid Street,  
Hamilton HM-11,  
Bermuda  
Phone: +1-441-278-2800  
Website: [www.quovadisglobal.com](http://www.quovadisglobal.com)  
Electronic mail: [compliance@quovadisglobal.com](mailto:compliance@quovadisglobal.com)

*Mailing Address:*

QuoVadis Limited  
Suite 1640  
48 Par-La-Ville Road  
Hamilton HM-11  
Bermuda

**Netherlands**

QuoVadis Trustlink BV  
Maliesingel 22  
3581 BG Utrecht  
The Netherlands  
Phone: +31 (0) 30 232-4320

**Switzerland**

QuoVadis Trustlink Schweiz AG  
Teufenerstrasse 11  
9000 St. Gallen  
Switzerland  
Phone: +41-71-272-60-60

**United Kingdom**

QuoVadis Online Security Limited  
8 Hayters Court, Brockenhurst Business Park  
Grigg Lane, Brockenhurst  
Hampshire SO42 7PG  
United Kingdom  
Phone: +44 (0) 1590-624400

**3. TIME-STAMP TOKEN TYPES AND USAGE**

The QV-TSA aims to deliver time-stamping services used in support of qualified electronic signatures (i.e., in accordance with article 5.1 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures). However, QV time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time. The baseline profile uses SHA-1 with RSA encryption and 2048 bit key size for signature creation. Acceptable Time Stamp Request Hashes include SHA-1, SHA-256, SHA-384 and SHA-512. The QuoVadis digital signature on the Time-Stamp Token (TST) has a validity period of ten years. Refer to section 6 below for information on how to verify a TST.

**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  $\pm 1$  second of a trusted UTC time source. If a trusted UTC time source can not 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 use the software toolkit provided by QuoVadis to request and retrieve time-stamps from the TSA, unless otherwise specifically authorised in writing. When retrieving a Time-Stamping Token (TST), subscribers must verify that the TST has been correctly signed and that the private key used to sign the time-stamp token is valid. Refer to the QuoVadis Time-Stamping Authority Subscriber Agreement and the QV-TSP/PS for additional obligations.

**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 is not listed on the QuoVadis Certificate Revocation List (CRL) at <http://crl.quovadisglobal.com/qvrca.crl>. 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 TS 102 023.

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.

**7. 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.

**8. APPLICABLE AGREEMENTS AND PRACTICE STATEMENT**

See the QV-TSP/PS and the QuoVadis CP/CPS at <http://www.quovadisglobal.com/repository>.

**9. 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.

**10. REFUND POLICY**

QuoVadis does not refund fees for time-stamp services.

**11. 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 article 5.1 of the European Directive), as well as under applicable Swiss, Dutch and Bermuda law 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 referred to an arbitration tribunal in the manner set out in the QuoVadis CP/CPS.

**12. TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT**

The QV-TSA has been certified for conformance to ETSI TS 101.023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities* and ETSI TS 101.861, *Time-stamping Profile* by KPMG AG.

In addition, QuoVadis maintains several accreditations and certifications of its Public Key Infrastructure. These include:

- **WebTrust for Certification Authorities.** The WebTrust seal of assurance for Certification Authorities symbolises to potential relying parties that a qualified practitioner has evaluated the Certification Authority's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities, and has issued a report with an unqualified opinion indicating that such principles are being followed. This audit is performed on an annual basis by Ernst & Young.
- **Qualified Certification Service Provider (Switzerland).** QuoVadis is entitled to issue and administer qualified electronic certificates in accordance with Swiss law. This includes certification to SR 943.03 (ZertES), ETSI TS 101.456 (Policy requirements for Digital Certification Authorities issuing Qualified Digital Certificates) and other standards. This audit is performed on an annual basis by KPMG.
- **Authorised Certification Service Provider (Bermuda).** QuoVadis is entitled to issue accredited certificates under the requirements of the Bermuda Electronic Transactions Act 1999.