QuoVadis

Time-Stamping Authority (TSA)
Disclosure Statement

OIDs:  1.3.6.1.4.1.8024.0.2000.6
Effective Date:  20 November, 2020
Version:  1.8
Important Notice about this Document

This document is the Time-Stamping Authority (TSA) Disclosure Statement of QuoVadis Limited (QuoVadis), a company of DigiCert, Inc. The purpose of this document is to summarise key aspects of the QuoVadis TSA for the benefit of Subscribers and Relying Parties.

This document does not substitute or replace the QuoVadis Time-Stamp Policy/Practice Statement (QV-TSP/PS) or the Certificate Policy/Certification Practice Statement (CP/CPS) which may be found at https://www.quovadisglobal.com/repository.

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 and any other person. Any person seeking to rely on Time-stamps must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with QuoVadis and its business.

This document is controlled and managed under the authority of the QuoVadis Policy Management Authority. The date on which this version of the Time-stamp Policy becomes effective is indicated on this document. The most recent effective copy of this Time-stamp Policy supersedes all previous versions. No provision is made for different versions of this Time-stamp Policy to remain in effect at the same time.

Version Control:

<table>
<thead>
<tr>
<th>Author</th>
<th>Date</th>
<th>Version</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>QuoVadis PMA</td>
<td>21 March 2006</td>
<td>1.0</td>
<td>Initial Draft based on ETSI TS102 023 model TSA disclosure statement.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>23 June 2008</td>
<td>1.1</td>
<td>Updates to URLs and updates based on ETSI TS102 023 model TSA disclosure statement.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>29 June 2010</td>
<td>1.2</td>
<td>Updates to algorithms.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>11 October 2010</td>
<td>1.3</td>
<td>Updates to include more detail on validity period of TSA certificate.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>25 May 2012</td>
<td>1.4</td>
<td>Updates for trusted time source and supported Algorithms.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>2 June 2017</td>
<td>1.6</td>
<td>Updates for new Swiss TSA Certificates.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>11 October 2019</td>
<td>1.7</td>
<td>Updates for new EU and Swiss TSA Certificates. Updates for accuracy.</td>
</tr>
<tr>
<td>QuoVadis PMA</td>
<td>20 November 2020</td>
<td>1.8</td>
<td>Editorial changes for alignment to ETSI EN 319 421, update to TSU information, change to QuoVadis Master Services Agreement/Subscriber Agreement.</td>
</tr>
</tbody>
</table>
**TABLE OF CONTENTS**

1. ENTIRE AGREEMENT ..................................................................................................................................................... 1
2. TSA CONTACT INFORMATION ................................................................................................................................... 1
3. TIME-STAMP TYPES AND USAGE ............................................................................................................................. 1
4. RELIANCE LIMITS ............................................................................................................................................................ 2
5. OBLIGATIONS OF SUBSCRIBERS ............................................................................................................................... 2
6. OBLIGATIONS OF RELYING PARTIES .......................................................................................................................... 3
   6.1. Qualified Electronic Time-stamp ............................................................................................................................ 3
   6.2. Long term Verification of Time-stamps .................................................................................................................. 3
7. RETENTION OF EVENT LOGS ..................................................................................................................................... 3
8. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY ........................................................................ 3
9. APPLICABLE AGREEMENTS AND PRACTICE STATEMENT ....................................................................................... 4
10. PRIVACY POLICY ............................................................................................................................................................ 4
11. REFUND POLICY .............................................................................................................................................................. 4
12. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION .................................................................................. 4
13. TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT ............................................................................ 4
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 https://www.quovadisglobal.com/repository.

2. TSA CONTACT INFORMATION
The QV-TSA is operated by QuoVadis Limited.
Website: https://www.quovadisglobal.com
Repository: https://www.quovadisglobal.com/repository
Customer complaints email: qvcomplaints@digicert.com

<table>
<thead>
<tr>
<th>Country</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
</table>
| Bermuda   | 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)  
Schaliënhoedvedreef 20T  
2800 Mechelen  
Belgium  
Phone: +32 15 79 65 21 |                |
| Germany   | QuoVadis Trustlink Deutschland GmbH  
Ismaninger Str. 52  
D-81675 München  
Germany  
Phone: +49-89-540-42-45-42 |                |
| Netherlands | QuoVadis Trustlink BV  
Nevelgaarde 56 noord  
3436 ZZ Nieuwegein  
The Netherlands  
Phone: +31 (0) 30 232-4320 |                |
| Switzerland | QuoVadis Trustlink Schweiz AG  
Poststrasse 17, Postfach  
9001 St. Gallen  
Switzerland  
Phone: +41-71-272-60-60 |                |
| United Kingdom | QuoVadis Online Limited  
2 Harbour Exchange Square  
London, E14 9GE  
United Kingdom  
Phone: +44 (0) 333-666-2000 |                |

3. TIME-STAMP 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.

QuoVadis Time-stamps are compliant with RFC 3161. The cryptographic algorithms and key lengths used by the QV-TSA comply with ETSI EN 319 422 and TAV:

- Acceptable Time-stamp request hashes: SHA-256, SHA-384, SHA-512
- Signature: sha256WithRSAEncryption (minimum 2048 bit key)

TSU Public Key Certificates have a validity period of up to five years.

Refer to Section 6 (Obligations of Relying Parties) of this document for information on how to verify a Time-stamp. Use of the QV-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 Time-stamps on behalf of the TSA. Each TSU has a different key. Refer to the “QuoVadis TSAs” section of https://www.quovadisglobal.com/repository for a complete list of QuoVadis TSUs.

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

<table>
<thead>
<tr>
<th>QuoVadis TSU Subject</th>
<th>TSU Issuer</th>
<th>Status</th>
</tr>
</thead>
</table>
| CN = eutsa01.quovadisglobal.com  
CN = eutsa02.quovadisglobal.com  
CN = eutsa03.quovadisglobal.com | QuoVadis Time-Stamping Authority  
CA G1 | Qualified Electronic Time-stamp  
According to eIDAS -  
Netherlands  
https://webgate.ec.europa.eu/tl-browser/#/tl/NL/9/14 |
| CN = betsa01.quovadisglobal.com  
CN = betsa02.quovadisglobal.com  
CN = betsa03.quovadisglobal.com | QuoVadis Belgium Issuing CA G2 | Belgium  
Not featured on a Trusted List |
| CN = chtsa01.quovadisglobal.com  
CN = chtsa02.quovadisglobal.com  
CN = chtsa03.quovadisglobal.com | QuoVadis Time-Stamping Authority  
CA G1 | Qualified Electronic Time-stamp  
According to ZertES -  
Switzerland |

4. RELIANCE LIMITS

QuoVadis does not set reliance limits for Time-stamp services, however reliance limits may be set by applicable law or by agreement.

The QV-TSA assures time with ±1 second or better of a trusted UTC time source. If a trusted UTC time source cannot be acquired the time stamp will not be issued. The time included in a Time-stamp is the time of processing by the TSU, not the time of submission nor of acceptance.

5. OBLIGATIONS OF SUBSCRIBERS

Subscribers must verify that the Time-stamp has been correctly signed and check that the Private Key used to sign the Time-stamp has not been revoked. The Subscriber shall use the QuoVadis Time-Stamping service in accordance with the QV-TSP/PS, CP/CPS, ETSI EN 319 421 and the relevant provisions in ETSI EN 319 422.
Subscribers must use secure cryptographic functions for Time-stamping requests. Subscriber obligations are also defined in the relevant QuoVadis Agreements (including the Master Services Agreement, Subscriber Agreement, Terms of Use, and Relying Party Agreement as applicable).

6. **OBLIGATIONS OF RELYING PARTIES**

Before placing any reliance on a Time-stamp, Relying Parties must verify that the Time-stamp has been correctly signed and that the Private Key used to sign the Time-stamp has not been revoked. The Relying Party should take into account any limitations on usage of the Time-stamp indicated by this QV-TSP/PS and any other reasonable precautions.

During the TSU Certificate validity period, the status of the Private Key can be checked using the relevant QuoVadis CRL. QuoVadis CA and TSU Certificates are published at [https://www.quovadisglobal.com/repository](https://www.quovadisglobal.com/repository).

Note that QuoVadis operates multiple TSU, signed by different QuoVadis Issuing CAs aligned with different jurisdictions or regulations. See Section 3 (Time-stamp Types and Usage) of this document.

6.1. **QUALIFIED ELECTRONIC TIME-STAMP**

When a Time-stamp is claimed to be a Qualified Electronic Time-stamp as per Regulation (EU) No 910/2014, the TSU Public Key Certificate will be issued by a CA listed on an EU Trusted List.

A Relying Party is expected to use a Trusted List to establish whether the TSP and the TSU are Qualified. If the Public Key of the TSU is listed in the Trusted List and the TSP it represents is a Qualified Time-stamping service, then the Time-stamps issued by this TSU can be considered as Qualified.

The qcStatement "esi4-qstStatement-1" as defined in ETSI EN 319 422 can be used to indicate a Qualified Electronic Time-stamp.

6.2. **LONG TERM VERIFICATION OF TIME-STAMPS**

In accordance with Annex D of ETSI EN 319 421, verification of a Time-stamp can still be performed after the end of the validity period of the Certificate, if at the time of verification:

- the TSU Private Key has not been compromised;
- the hash algorithm, signature algorithm and signature key size are still supported by this QV-TSP/PS.

Technical developments can reduce the security value of Time-stamped data. Validity may be maintained by applying an additional Time-stamp to protect the integrity of the previous one. Alternatively the Time-stamped data may be placed in secure storage.

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 the following obligations to QV-TSA Subscribers:

- To operate in accordance with this QV-TSP/PS and the CP/CPS;
- To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second or better;
- Undergo internal and external reviews to assure compliance with relevant legislation and QuoVadis policies and procedures; and
- To provide high availability access to QV-TSA systems except in the case of planned technical interruptions, loss of time synchronization, or Certificate verification issues.

Information regarding limitations of the service, Subscribers’ obligations, information for Relying Parties, or limitations of liability may be found in QuoVadis Agreements (including the Master Services Agreement, Subscriber Agreement, Terms of Use, and Relying Party Agreement as applicable).
9. APPLICABLE AGREEMENTS AND PRACTICE STATEMENT
See the QV-TSP/PS and the QuoVadis CP/CPS at https://www.quovadisglobal.com/repository.

10. PRIVACY POLICY
The QV-TSA complies with applicable regulations and legal requirements (including eIDAS and ZertES), as well as the requirements of the QuoVadis Privacy Policy (see https://www.quovadisglobal.com/privacy-policy/).

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

12. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION
Any controversy or claim relating to the QV-TSA shall be addressed according to Section 9.13 (Dispute Resolution Procedures) and Section 9.13 (Governing Law) of the CP/CPS.

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