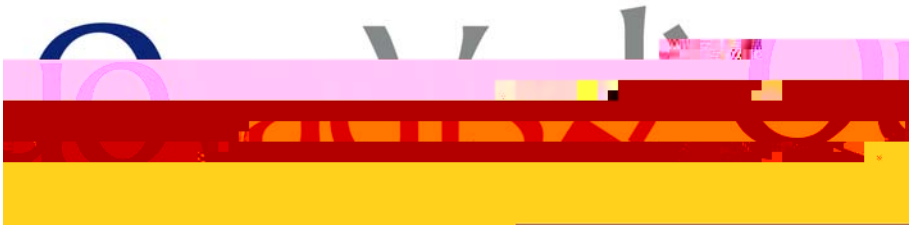

QUOVADIS TIME-STAMP POLICY/PRACTICE STATEMENT

OID: 1.3.6.1.4.1.8024.0.2000.6
Effective Date: 25 May, 2012
Version: 2.3

Important Note About this Document

The QuoVadis Time-Stamp Policy and the QuoVadis Time-Stamp Practice Statement have been merged into one document, the QuoVadis Time-Stamp Policy/Practice Statement (QV-TSP/PS). This QV-TSP/PS contains an overview of the policies, practices and procedures that QuoVadis employs for its operation as a Time-stamp Authority. 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.

Contact Information:

Corporate Offices:
QuoVadis Limited
3rd Floor Washington Mall
7 Reid Street,
Hamilton HM-11,
Bermuda

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

Website: http://www.quovadisglobal.com/
Electronic mail: compliance@quovadisglobal.com

Version Control

Author	Date	Version	Comment
Stephen Davidson	22 December 2005	0.1	Initial Draft

Table of Contents

3. Definitions and Abbreviations

3.1 Definitions

"Certificate Policy/Certification Practice Statement" or "CP/CPS" means is a publicly available document that details the QuoVadis PKI and describes the practices employed in issuing Digital Certificates.

"Time-Stamp Authority" or **"TSA"** means a trusted authority which issues time-stamp tokens.

"Time-Stamp Policy/Practice Statement" or "**QV-TSP/PS**" (this document) means a set of rules that indicate the applicability of a time-stamp token to a particular community or class of application with common security requirements.

"Time-Stamp Token" or **"TST"** means a data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.

"Time-Stamp Unit" or **"TSU"** means a set of hardware and software which is managed as a unit and has a single private signing key active at a time.

"TSA Disclosure Statement" means an overview of the policies and pr

4. General Concepts

4.1 Time-stamping Services

Time-stamping services include the following components:

Time-stamping provision: the technical component that issues the Time-Stamp Tokens (TSTs).
Time-stamping management: the service component that monitors and controls the time-stamping operation, including synchronization with the reference UTC time source, according to the QV-TSP/PS.

QuoVadis adheres to the international standards in section 2 *(References)* of this document to increase the trustworthiness of the time-stamping services for both Subscribers and Relying Parties.

4.2 Time-stamping Authority

The TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue secure TSTs. The QV-TSA takes overall responsibility for the provision of time-stamping services identified in section 4.1.

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.

QuoVadis Limited operates the QV-TSA as part of its public key infrastructure (PKI). The QV-TSA is identified in the Digital Certificates used in the time-stamping service.

4.3 Subscribers and Relying Parties

Subscribers are entities that hold a service contract with QuoVadis and have agreed to the QuoVadis Time-Stamping Authority Subscriber Agreement. Organisations that are Subscribers are responsible for the activities of their associated users and Relying Parties and are expected to inform them about the correct use of time-stamps and the conditions of the QV-TSP/PS. Subscribers must use a method or software toolkit approved by QuoVadis to create time-stamps, unless otherwise specifically authorised in writing by QuoVadis.

4.4 TSA Policy and Practices

4.4.1 Purpose

The QuoVadis Time-Stamp Policy ("what is adhered to") and the QuoVadis Time-Stamp Practice Statement ("how it is adhered to") have been merged into one document, the QV-TSP/PS. The This QV-TSP/PS specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services as defined by the standards in section 2 *(References)* of this document.

For additional detail on the QV-TSA, refer to section 7.1 *(Practice and Disclosure Statements)* of this document. All QuoVadis policies and practices are under the control of the QV Policy Management Authority.

4.4.2 Level of Specificity

This QV-TSP/PS extends the CP/CPS which regulates the operation of the QV-PKI and associated non-repudiation services. The QV-TSP/PS and CP/CPS are public documents and may be downloaded at http://www.quovadisglobal.com/repository.

4.4.3 Approach

The QV-TSP/PS establishes the general rules concerning the operation of the QV-TSA. Additional internal documents define how QuoVadis meets the technical, organizational, and procedural requirements identified in the QV-TSP/PS. These documents may be provided only under strictly controlled conditions.

5. Time-stamp Policy

5.1 Overview

This TSP defines a set of processes for the trustworthy creation of time-stamp tokens in accordance with ETSI TS 102.023. The private keys and the TSU meet the technical specifications of ETSI TS 101.861 and RFC 3161.

The QV-TSA signs time-stamps using private keys that are reserved specifically for that purpose. Each TST contains an identifier to the applicable policy, and TSTs are issued with time accurate to ±1 second of UTC.

Time-stamps are requested by means of either the Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP), as described by RFC 3161.

The URL for the QV-TSP/PS is:

otherwise. During the TSU Certificate validity period, the status of the private key can be checked using the QuoVadis CRL (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.

6.4 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.

7. TSA Practices

The provision of a time-stamp token in response to a request is at the discretion of QuoVadis depending on agreements with the Subscriber.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice Statement

This QV-TSP/PS establishes the general rules concerning the operation of the QV-TSA. The CP/CPS and additional internal documents define how QuoVadis meets the technical, organizational, and procedural requirements identified in the QV-TSP/PS.

The QV-TSP/PS, the CP/CPS, TSA Disclosure Statement, and other public documents may be found at http://www.quovadisglobal.com/repository. Internal documents may be provided only under strictly controlled conditions. Notice will be given of changes to this QV-TSP/PS.

QuoVadis conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures. Additional detail may be found in section 5.4.8 *(Vulnerability Assessment)* of the CP/CPS.

The QV-TSP/PS and CP/CPS identify the obligations of external organizations supporting the TSA services including the applicable policies and practices.

The QuoVadis Policy Management Authority has responsibility for maintaining and approving all QV-PKI policies and practices according to the terms of section 1.5 *(Policy Administration)* of the CP/CPS. QuoVadis management has responsibility to ensure that the practices are properly implemented.

7.1.2 TSA Disclosure Statement

The TSA Disclosure Statement may be found at http://www.quovadisglobal.com/repository along with other important documents associated with use of the QV-PKI. This document discloses to all Subscribers and potential Relying Parties the terms and conditions regarding use of QuoVadis time-stamping services. Summarised elements of the QV-TSA Disclosure Statement are below:

> The QV-TSA is a service of QuoVadis limited, which is certified under Swiss ZertES as a qualified certification service provider, and under the Bermuda ETA as an Authorised Certification Service Provider.
> Contact information for QuoVadis and the QV-TSA is provided in section 1.5.2 *(Contact Per7l(menD-.088.5 0 TTJ-411.6 178.56*

7.3 Time-stamping

7.3.1 Time-stamp Token

QuoVadis has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in section 2 of this document, each TST includes:

a representation (e.g., hash value) of the datum being time-stamped as provided by the requestor;
a unique serial number that can be used to both order TSTs and to identify specific TSTs;
an identifier for the time-stamp policy;
the time calibrated to within 1 second

systems access management controls. Additional information is provided in section 5 *(Facility, Management, and Operational Controls)* of the CP/CPS and section 6 *(Technical Security Controls)* of the CP/CPS.

7.4.7 Trustworthy Systems Deployment and Maintenance

The QV-TSA uses trustworthy systems that are protected against modification. The systems deployment and maintenance controls for the QV-TSA are incorporated within the overall QV-PKI systems deployment and maintenance controls. Additional information is provided in section 6 *(Technical Security Controls)* of the CP/CPS.

7.4.8 Compromise of TSA Services

In the event of compromise of a TSU private key, QuoVadis will follow the procedures outlined in section 5.7 *(Compromise and Disaster Recovery)* of the CP/CPS. This includes revoking the relevant Certificate and adding it to the QuoVadis CRL. The TSU will not issue time-stamps if its private key is not valid.

The TSU will not issue time-stamps if its clock is outside the declared accuracy from reference UTC, until steps are taken to restore calibration of time. As described in section 7.4.11 *(Recording of Information Concerning Operation of Time-stamping Services)* of this document, the QV-TSA maintains audit trails to discriminate between genuine and backdated tokens.

7.4.9 TSA Termination

In the case of termination of the QV-TSA, QuoVadis will follow the procedures in section 5.8 *(Certificate Authority and/or Registration Authority Termination)* of the CP/CPS and also more detailed internal QuoVadis termination procedures. These include at a minimum informing Subscribers, revoking TSU Certificates, and transferring obligations to a reliable party for maintaining event log and audit archives as well as access to private keys.

7.4.10 Compliance with Legal Requirements

The QV-TSA complies with applicable legal requirements (ZertES and the ETA), as well as the requirements of the European data protection Directive [Dir 95/46/EC]. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Information contributed by users to the TSA shall be completely protected from disclosure unless with their agreement or by court order or other legal requirement.

7.4.11 Recording of Information Concerning Operation of Time-stamping Services

QuoVadis maintains records of all relevant information concerning the operation of the QV-TSA for a period of 11 years, in accordance with the QuoVadis business practices. Records are time-stamped to protect data integrity and moved to a protected server for storage and subsequent archiving. Records are treated as confidential in accordance with the CP/CPS. No personal data relating to Subscribers is transmitted between jurisdictions.

Records concerning the operation of time-stamping services are available at the request of Subscribers or if required by court order or other legal requirement. The QV-TSA maintains records, including precise time, of:

Time-stamp requests and created time-stamps
Events related to TSA administration (including Certificate management, key management, and clock synchronisation).
Events relating to the life-cycle of TSU keys and Certificates.

7.5 Organisational

The QuoVadis organisational structure, policies, procedures and controls apply to the QV-TSA. QuoVadis organisational procedures fulfil the standards in section 2 *(References)* of this document, in particular ETSI TS 102.023. Important policy and practice documents for the QV-PKI are available at http://www.quovadisglobal.com/repository. Other internal procedural documents may be provided only under strictly controlled conditions.