QUOVADIS TIME-STAMP POLICY

OID: 1.3.6.1.4.1.8024.0.2000.6
Effective Date: 21 March, 2006
Version: 1.0
Document Name: QV_TSApolicy_v1

Important Note About this Document

The QuoVadis Time-stamp Policy contains an overview of the 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:	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

Website: www.quovadis.bm
Electronic mail: policy@quovadis.bm

Version Control

Author	Date	Version	Comment
Stephen Davidson	22 December 2005	0.1	Initial Draft
Stephen Davidson	12 January 2006	0.2	Reviewed Draft
Stephen Davidson	16 February 2006	0.3	Reviewed Draft
Stephen Davidson	20 March 2006	0.4	KPMG Comments
QuoVadis PMA	21 March 2006	1.0	Approved

Table of Contents

Introduction
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (European Directive) defines "certification service provider" in article 2.11 as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures". A time-stamping authority is such a certification service provider.

Electronic signatures are used to add security by creating a tamperproof cryptographic seal around electronic data. Once a datum is signed, any change to its content will cause the electronic signature to fail, alerting the user. Electronic signatures may be used in several ways:

- Individual electronic signatures support the integrity of electronic records by declaring WHO signed WHAT (in other words, who created particular content or changes).

- Time-stamps use electronic signatures, incorporating the time from an accurate source, to confirm WHAT happened WHEN.

Individual signatures may be used independently – or together with time-stamps – to increase the trustworthiness of electronic records and transactions.

1.   Scope
The QuoVadis Time-stamping Authority (QV-TSA) uses public key infrastructure and trusted time sources to provide reliable, standards-based time-stamps. This QuoVadis Time-stamp Policy (QV-TSP) defines the operational and management practices of the QV-TSA such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

The QV-TSP 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 and Bermuda law and regulations. However, QuoVadis time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The structure and contents of this policy are laid out in accordance with ETSI TS 101.023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.* The QV-TSP is administered and approved by the QuoVadis Policy Management Authority, and should be read in conjunction with the current QuoVadis Certification Practice Statement (QV-CPS).

2.   References
The following documents contain provisions which are relevant to the QV-TSP.

[1]   ETSI TS 101.456, Policy Requirements for Certification Authorities Issuing Qualified Certificates.
[2]   ETSI TS 101.861, Time-stamping Profile.
[3]   ETSI TS 102.023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.
[4]   ETSI TS 102.176.1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms.
[5]   QuoVadis Certification Practice Statement (QV-CPS), OID 1.3.6.1.4.8024.0.1
[6]   RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures.
[7]   RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
[8]   SR 943.03 (ZertES), Switzerland, Electronic Signature Law.
[9]   SR 943.032 (VZertES), Switzerland, Swiss Electronic Signature Ordinance.
[10]   SR 943.032.1 (TAV), Switzerland, Technical and Administrative Prescriptions for Certification Service Providers.
[11]   Electronic Transactions Act (ETA), Bermuda, Certification Service Provider Regulations.

3. Definitions and Abbreviations
3.1 Definitions

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

"Time-stamp policy" (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 practices of a TSA that require particular emphasis to subscribers and relying parties.

"TSA Practice Statement" defines the practices that a TSA employs in issuing time-stamp tokens.

"Relying party" means an entity which relies on a time-stamp token and has entered into the QV-TSA Relying Party Agreement.

"Subscriber" means an entity (an individual or organisation) which requires the services provided by a TSA and has entered into the QV-TSA Subscriber Agreement.

"Coordinated Universal Time" or **"UTC"** means the time scale, based on the second, as defined by the International Telecommunications Radio Committee (ITU-R) TF.460-5 and roughly corresponding to Greenwich Mean Time (GMT).

"UTC(k)" means a time scale realized by a laboratory "k" as defined in Bureau International des Poids et Mesures (BPIM) Circular T and kept in close agreement with UTC.

Additional definitions are provided in the QV-CPS.

3.2 Abbreviations

Term	Description
CP	Certification Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
ETA	Bermuda Certification Service Provider Regulations, April 2002
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Modules
PKI	Public Key Infrastructure
QV	QuoVadis
TSA	Time-stamping Authorities
TST	Time-stamping Token
TSU	Time-stamping Unit
UTC	Coordinated Universal Time
VZertES	Swiss Electronic Signature Ordinance, 3 December 2004
ZertES	Swiss Electronic Signature Law, 19 December 2003

4. General Concepts
4.1 Time-stamping Services
Time-stamping services include the following components:

- Time-stamping provision: the technical component that issues the 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.

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 time-stamp tokens (TST). 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-stamp 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 QV-TSA terms and conditions. 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. Subscribers must use the software toolkit provided by QV to create time-stamps, unless otherwise specifically authorised in writing by QV.

4.4 TSA Policy and Practices
4.4.1 Purpose
The QV-TSP (this document) specifies a time-stamp policy to meet general requirements for trusted time-stamping services as defined by the standards in section 2 *References* of this document.

The QV_TSP states in general "what is adhered to", while the QV-TSA practice statement states "how it is adhered to", (for example by defining rge processes used to create time-stamps and maintain clock accuracy).

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 extends the QV-CPS which regulates the operation of the QV-PKI and associated non-repudiation services. The QV-TSP and QV-CPS are public documents and may be downloaded at http://www.quovadis.bm/policies/.

4.4.3 Approach
The QV-TSP 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. 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 line 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 TSA is: http://www.tsa01.quovadisoffshore.com.

5.2   Identification
The object-identifier (OID) of the baseline QV-TSP is: 1.3.6.1.4.1.8024.0.2000.6

This OID is referenced in every QV issued time-stamp, and the QV-TSP is available to both Subscribers and Relying Parties.

The OID for the QV-CPS is: 1.3.6.1.4.8024.0.1

5.3   User Community and Applicability
The user community for QuoVadis time-stamps includes only Subscribers and their Relying Parties. All Subscribers are automatically deemed to be Relying Parties. QuoVadis does not provide public time-stamp services.

QuoVadis does not impose restrictions on applicability of its time-stamps, with the exception of prohibited uses outlined in section 1.4.2 *Prohibited Certificate Usage* of the QV-CPS.

The QV-TSP aims to deliver time-stamps that correspond to the requirements for qualified electronic signatures under ZertES. However, QV time-stamps may be applied to any application requiring proof that a datum existed before a particular time.

5.4   Conformance
QuoVadis references the policy identifier in section 5.2 *Identification* of this document in all time-stamps to indicate conformance with this policy. QuoVadis is subject to periodic independent internal and external reviews to demonstrate that the QV-TSA meets its obligations defined in section 6.1 *TSA Obligations* and has implemented appropriate controls in line with section 7 *TSA Practices*.

6.   Obligations and Liability
6.1   TSA Obligations

6.1.1   General Obligations
QuoVadis Limited operates the QV-TSA and assumes responsibility that the requirements of section 7 *TSA Practices* of this document - as well as the provisions of ZertES, its associated TAV regulations, and the ETA - are implemented as applicable to the selected trusted time-stamp policy.

QuoVadis is a party to the mutual agreements and obligations between the TSA, Subscribers, and Relying Parties. The QV-TSP and QV-CPS are integral components of these agreements.

6.1.2 TSA Obligations Towards Subscribers
QuoVadis undertakes the following obligations to TSA Subscribers:

- To operate in accord with the QV-TSP, the QV-CPS, and other relevant operational policies and procedures.
- To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second.
- Undergo internal and external reviews to assure compliance with relevant legislation and internal QuoVadis policies and procedures.
- To provide high availability access to QV-TSA systems except in the case of planned technical interruptions, loss of time synchronization, and causes outlined in section 9.8.3 *Excluded Liability* of the QV-CPS.

6.2   Subscriber Obligations
Subscribers must verify that the time-stamp token has been correctly signed and check the QV CRL to confirm that the private key used to sign the time-stamp token has not been compromised. Subscribers must use the software toolkit provided by QuoVadis to request and retrieve time-stamps from the TSA, unless otherwise specifically authorised in writing.

6.3   Relying Party Obligations
Before placing any reliance on a time stamp, subject to section 7.1.2 *TSA Disclosure Statement* of this document, relying parties must verify that the TST has been correctly signed and that the private key used to sign the TST has not been compromised until the time of verification. During the TSU certificate validity period, the status of the private key can be checked using the QV CRL. After expiry of the TSU certificate, the relying party should:

- Verify that the TSU private key is not listed on the QV CRL, and
- Verify that the cryptographic hash function used in the TST is still considered secure, and
- Verify that the cryptographic algorithm and key size used by the TSU is still considered secure.

6.4   Liability
QuoVadis undertakes to operate the QV-TSA in accordance with the QV-TSP, the QV-CPS, and the terms of service level 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 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 *Liabilities* of the QV-CPS.

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

7.1   Practice and Disclosure Statements
7.1.1   TSA Practice Statement
The QV-TSP establishes the general rules concerning the operation of the QV-TSA. The QV-CPS and additional internal documents define how QuoVadis meets the technical, organizational, and procedural requirements identified in the QV-TSP.

The QV-TSP, the QV-CPS, TSA Disclosure Statement, and other public documents may be found at http://www.quovadis.bm/policies. Internal documents may be provided only under strictly controlled conditions.

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 QV-CPS.

The QuoVadis Policy Management Authority has responsibility for maintaining and approving all QV-PKI policies and practices according to the terms of section 1.6 *Policy Administration* of the QV-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.quovadis.bm/policies 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.

- 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 1.6.5 *Contact Person* of the QV-CPS.

- Each time-stamp token issued by the QV-TSA contains the policy object-identifier contained in section 5.2 *Identification* of this document.

- The cryptographic algorithms and key lengths used by the QV-TSA comply with ETSI TS 101.861 and TAV and are currently:

  - Hash: SHA-1 or MD5
  - Signature: sha1WithRSAEncryption, 2048 bit key

- QuoVadis does not set reliance limits for time-stamp services beyond those outlined in section 6.3 *Relying Party Obligations* of this document. QuoVadis will post public notice on its website if it determines that cryptographic algorithms and key lengths used in the QV-PKI are no longer considered secure.

- The QV-TSA assures time with ±1 second of a trusted UTC time source and will not issue time-stamps outside this declared accuracy.

- Subscriber obligations are described in section 6.2 *Subscriber Obligations* of this document.

- Relying Party obligations are described in section 6.3 *Relying Party Obligations* of this document.

- QuoVadis maintains secure records concerning the operation of the QV-TSA according to section 5.5 *Records Archival* of the QV-CPS.

- QuoVadis makes no express or implied representations or warranties relating to the availability or accuracy of the QV-TSA. 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 *Liabilities* of the QV-CPS.

- The applicable legal system and dispute resolution procedures relating to the QV-TSA are dealt with in the underlying Subscriber agreement.

- QV-TSA conformance with the applicable Time-stamp Policy is confirmed by the certification body of KPMG Klynveld Peat Marwick Goerdeler SA.

7.2   Key Management Life Cycle
7.2.1   TSA Key Generation
QuoVadis generates the cryptographic keys used in its TSA services under M of N control by authorised personnel in a secure physical environment. Additional information is provided in section 6.1 *Key Generation and Installation* of the QV-CPS. The keys are generated within TSU hardware security modules that are certified to FIPS 140-2 Level 3. Algorithms and key size are described in section 7.1.2 *TSA Disclosure* of this document.

7.2.2   TSU Private Key Protection
QuoVadis takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity. These include use of HSMs certified to FIPS 140-2 Level 3 to hold and sign with the keys.

7.2.3   TSU Public Key Distribution
Digital certificates used in the QuoVadis TSA are issued by the QV-PKI according to certificate policies which provide a level of security equivalent to this time-stamping policy. Additional information is provided in section 6.1 *Key Generation and Installation* of the QV-CPS.

7.2.4   Rekeying TSU's Key
TSU private signing keys are replaced before the end of their validity period, (i.e., when their algorithm or key size are determined to be vulnerable). Additional information is provided in section 4.6 *Certificate Renewal* and section 4.7 *Certificate ReKey* of the QV-CPS.

7.2.5   End of TSU Key Life Cycle
TSU private signing keys are replaced upon their expiration. The TSU rejects any attempt to issue time-stamps once a private key has expired. After expiry, private keys are destroyed.

7.2.6   Life Cycle Management of the Cryptographic Module used to Sign Time-stamps
QuoVadis has in place procedures to ensure that hardware security modules intended for non-repudiation services are not tampered with in shipment or storage. Acceptance testing is performed to verify that cryptographic hardware is performing correctly.   Installation and activation is performed only by M of N authorised personnel, and the devices operate in a physically secured environment. Private keys are erased from modules when they are removed from service according to manufacturer instructions. Additional information is provided in section 6.6 *Life Cycle Technical Controls* of the QV-CPS.

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 of UTC, traceable to a UTC(k) source
- an electronic signature generated using a key used exclusively for time-stamping
- an identifier for the TSA and the TSU

The QuoVadis TSUs maintain audit logs for all calibrations against the UTC(k) references, and will not issue TSTs when the time is out of the stated accuracy.

7.3.2   Clock Synchronization with UTC

The QuoVadis TSA provides time with ±1 second of a trusted UTC(k) time source. The QuoVadis TSUs have technical measures in place to ensure that their time is synchronized with UTC within the declared accuracy. The QV TSUs use DS/NTP, a mutually authenticated extension of the Network Time Protocol (NTP), to secure synchronizations with the UTC(k) reference and to provide audit records that the time in a given TST is accurate.

TSU clocks are protected within the HSMs and are periodically recalibrated against the reference UTC time source. TSU clocks are also able to monitor time drift outside preset boundaries and request additional recalibrations as needed. If the TSU clock drifts outside the declared accuracy, and recalibration fails, the TSA will not issue time-stamps until correct time is restored. Manual administration of the TSU clock requires M of N authorized personnel.

7.4   TSA Management and Operation
7.4.1   Security Management

QuoVadis has an active security management programme designed to document, implement, and maintain adequate security provisions for the QV-PKI according to best practice and the requirements of relevant standards. Additional information is provided in section 5 *Facility, Management, and Operational Controls* and section 6 *Technical Security Controls* of the QV-CPS.

7.4.2   Asset Classification and Management

In order to ensure that information and other assets receive appropriate security treatment, QuoVadis maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis. Additional information is provided in section 6.6 *Life Cycle Technical Controls* of the QV-CPS.

7.4.3   Personnel Security

To enhance the trustworthiness of its PKI operations, QuoVadis maintains appropriate personnel practices fulfilling security best practice and the requirements of relevant standards. Additional information is provided in section 5 *Facility, Management, and Operational Controls* and section 6 *Technical Security Controls* of the QV-CPS.

7.4.4   Physical and Environmental Security

The QV-TSA is part of the QV-PKI, which operates from a resilient and secure hosting facility. PKI elements are hosted within a caged area, with controlled access to authorized personnel only. Additional information is provided in section 5 *Facility, Management, and Operational Controls* and section 6 *Technical Security Controls* of the QV-CPS.

7.4.5   Operations Management

The QV-PKI maintains extensive operational controls in compliance with ETSI TS 102.023. This documentation is not publicly available. QuoVadis undergoes internal and external reviews of compliance and the effectiveness of these controls.

7.4.6   System Access Management

QuoVadis maintains appropriate physical and logical access controls for affected facilities, hardware, systems, and information. Additional information is provided in section 5 *Facility, Management, and Operational Controls* of the QV-CPS.

7.4.7   Trustworthy Systems Deployment and Maintenance

Certificates for the time-stamp service are created in accordance with section 7.2.1 *TSA Key Generation* of this document, and change control procedures maintain appropriate levels of assurance.

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 QV-CPS. This includes revoking the certificate and adding it to the QV 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 QV-CPS. 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]. 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. 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 QV-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).

7.5   Organizational
The QV-TSA is part of the QV-PKI operated by QuoVadis Limited incorporated under the laws of Bermuda. QuoVadis security precautions fulfill the standards in section 2 *References* of this document, in particular ETSI TS 102.023. Many important policy and practice documents for the QV-PKI are available at http://www.quovadis.bm/policies/. Other internal procedural documents may be provided only under strictly controlled conditions.