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: www.quovadisglobal.com
Electronic mail: compliance@quovadisglobal.com

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
QuoVadis PMA	19 November 2007	1.1	Updates to reflect trusted time source, new URL
QuoVadis PMA	23 June 2008	2.0	Update to combine the Time-Stamp Policy and Practice Statement. Updates to reflect new URLs.

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/Practice Statement (QV-TSP/PS) 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-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. 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 QV-TSP/PS are laid out in accordance with ETSI TS 102.023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.* The QV-TSP/PS is administered and approved by the QuoVadis Policy Management Authority, and should be read in conjunction with the current QuoVadis Certificate Policy/Certification Practice Statement (CP/CPS).

2. References

The following documents contain provisions which are relevant to the QV-TSP/PS:

[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 Certificate Policy/Certification Practice Statement (CP/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

"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 practices of a TSA that require particular emphasis to subscribers and relying parties.

"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 CP/CPS.

3.2 Abbreviations

Term	Description
CP/CPS	Certificate Policy/ Certification 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 Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

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 URL for the QV TSA is: http://www.quovadisglobal.com/repository.

5.2 Identification

The object-identifier (OID) of the baseline QV-TSP/PS 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/PS is available to both Subscribers and Relying Parties.

The OID for the CP/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 CP/CPS.

The QV-TSP/PS 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

not been compromised until the time of verification. The Relying Party should take into account any limitations on usage of the time-stamp indicated by this QV-TSP/PS and any other precautions prescribed in this agreement or otherwise. During the TSU certificate validity period, the status of the private key can be checked using the QV CRL (http://crl.quovadisglobal.com/qvica2.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 th

- 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 CP/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 CP/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. The personnel authorized to carry out this function shall be limited to those requiring to do so under QuoVadis practices. Additional information is provided in section 6.1 *(Key Generation and Installation)* of the CP/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 or higher to hold and sign with the keys. When TSU private keys are backed up, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The personnel authorized to carry out this function shall be limited to those requiring to do so under QuoVadis practices. Any backup copies of the TSU private signing keys are stored in an encrypted state (using an encryption key to create a “cryptographic wrapper” around the key).

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 CP/CPS.

7.2.4 Rekeying TSU's Key

TSU private signing keys are replaced before the end of their validity period, (i.e., when the algorithm or key size is determined to be vulnerable). Additional

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 UTC by calibration with the Sovereign Time service, which is

d) Personnel shall exercise administrative and management procedures and processes that are in line with the QuoVadis Information Security Policy

The following additional controls shall be applied to time-stamping management:

e) Managerial personnel shall be employed who possess:
   - knowledge of time-stamping technology;
   - knowledge of digital signature technology;
   - knowledge of mechanisms for calibration or synchronization the TSU clocks with UTC;
   - familiarity with security procedures for personnel with security responsibilities; and
   - experience with information security and risk assessment.

f) All QuoVadis personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA operations.

g) Trusted roles include roles that involve the following responsibilities:
   - Security Officers: Overall responsibility for administering the implementation of the security practices.
   - System Administrators: Authorized to install, configure and maintain the TSA trustworthy systems for time-stamping management.
   - System Operators: Responsible for operating the TSA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
   - System Auditors: Authorized to view archives and audit logs of the TSA trustworthy systems.

h) TSA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i) The TSA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

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 CP/CPS.

In particular:

a) For both the time-stamping provision and the time-stamping management:
   - physical access to facilities concerned with time-stamping services is limited to properly authorised individuals;
   - controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities; and
   - controls are implemented to avoid compromise or theft of information and information processing facilities.

b) Access controls are applied to the cryptographic modules to meet the requirements of security of cryptographic modules as identified in clauses 7.2.1 and 7.2.2.

c) The following additional controls have been applied to time-stamping management:
   - The time-stamping management facilities are operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.
   - Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations are outside this perimeter.
   - Physical and environmental security controls are implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The QuoVadis Information Security Policy (which includes systems concerned with time-stamping management) addresses the physical access control, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), protection against theft, breaking and entering and disaster recovery.
   - Controls are implemented to protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

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. The operations management controls for the QV-TSA are incorporated within the overall QV-PKI operations

management controls. Additional information in relation to Operations Management is provided in section 5 *(Facility, Management, and Operational Controls)* of the CP/CPS.

7.4.6 System Access Management

QuoVadis maintains appropriate physical and logical access controls for affected facilities, hardware, systems, and information. The systems access management controls for the QV-TSA are incorporated within the overall QV-PKI 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 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 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.