QUOVADIS TIME-STAMP POLICY

OID: 1.3.6.1.4.1.8024.0.2000.6
Effective Date: 21 March, 2006

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

Version Control

Author

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

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.

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.

- 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

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.