QUOVADIS TIME-STAMP POLICY/PRACTICE STATEMENT

OID: 1.3.6.1.4.1.8024.0.2000.6
Effective Date: 22 April, 2010
Version: 2 .1

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

Table of Contents

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

The URL for the QV-TSP/PSis: http://www.quovadisglobal.com/repository .

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

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

Time-stamps bearing this OID are trusted in the Adobe Approved Trust List (AATL).

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/PSaims 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, Subscrbers, and Relying Parties. The QV-TSP/PSand CP/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 accordance with this QV-TSP/PS, the CP/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 CP/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. Subscriber obligations are also defined in the Time-Stamping Authority Subscriber Agreement and the TSA Disclosure Statement.

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. 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 priv.BTe/TT0 1 Tf -il tutenp[(s)5(a-8(t)-T0 1 T05,Qes7di)-he.08 T

- 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. time

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 itself synchronized with multiple UTC(k) sources administered by different National Measurement Institutes. Audit and calibration records are maintained by both QuoVadis and Sovereign Time. The QuoVadis TSA ensures that clock synchronisation is maintained when a leap second occurs as notified by the appropriate body.

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 recalibrated at least twice daily 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. The QuoVadis Policy Management Authority is the body responsible for setting policies and practices for the overall PKI and is therefore responsible for defining the QuoVadis Information Security Policy. Additional information is provided in section 5 *(Facility, Management, and Operational Controls)* and section 6 *(Technical Security Controls)* of the CP/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 CP/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 CP/CPS

In particular:

a) QuoVadis employs personnel whom possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.
b) Security roles and responsibilities are summarized in job descriptions. Trusted roles, on which the security of the QuoVadis operation is dependent, are clearly identified in the CP/CPS.
c) QuoVadis personnel shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

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:
   - x knowledge of time- stamping technology;
   - x knowledge of digital signature technology;
   - x knowledge of mechanisms for calibration or synchronization the TSU clocks with UTC;
   - x familiarity with security procedures for personnel with security responsibilities; and
   - x 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) g)

12(nn)-8(e)]0 T(o)(d)--4(n)-8(t0(n)-8 -.2p(n)-80(n)-8p(-4( )1(i19(a)-1(y(EMC /LBody <8.49Tc 1.54(BDC Td (d (f))Tj 2e)8(j 52-4(i)-4(a678utd1(hor)2(r)r)i)