QuoVadis

Time-Stamp Policy/ Practice Statement

OID:	1.3.6.1.4.1.8024.0.2000.6
Effective Date:	2 June, 2017
Version:	2.5

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/
e-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.
QuoVadis PMA	22 April 2010	2.1	Updates to algorithms
QuoVadis PMA	11 October 2010	2.2	Updates to include more detail on validity period of TSA certificate
QuoVadis PMA	25 May 2012	2.3	Updates for trusted time source and supported algorithms
QuoVadis PMA	25 November 2016	2.4	Updates for eIDAS, Regulation (EU) No 910/2014. Updates for ETSI EN 319 421 and ETSI EN 319 422.
QuoVadis PMA	2 June 2017	2.5	Updates for new Swiss TSA Certificates

TABLE OF CONTENTS

Introduction

Regulation (EU) No 910/2014 ("eIDAS Regulation") includes requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time-stamps. Additionally, more specific requirements are identified in the Regulation for a specific class of TSP called a Qualified TSP. QuoVadis is a Qualified TSP.

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 Electronic 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 in accordance with the eIDAS regulation), as well as under other applicable national laws 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 EN 319 421, *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.* 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 EN 319.412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

[2] ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[3] ETSI EN 319.422, Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and Time-stamp Token Profiles.

[4] ETSI EN 319.421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[5] ETSI TS 102.176.1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms.

[6] ETSI TS 101.733, CMS Advanced Electronic Signatures

[7] QuoVadis Certificate Policy/Certification Practice Statement (CP/CPS)

[8] RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures.

[9] RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).

[10] SR 943.03 (ZertES), Switzerland, Electronic Signature Law.

[11] SR 943.032 (VZertES), Switzerland, Swiss Electronic Signature Ordinance.

[12] SR 943.032.1 (TAV), Switzerland, Technical and Administrative Prescriptions for Certification Service Providers.

[13] Electronic Transactions Act (ETA), Bermuda, Certification Service Provider Regulations.

[14] Regulation (EU) No 910/2014 of European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (eIDAS regulation)

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.

"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).

"Electronic time stamp" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

"Qualified electronic time stamp" means an electronic time stamp which meets the following requirements:

a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

b) it is based on an accurate time source linked to Coordinated Universal Time; and

c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

"Relying party" means an entity (an individual or organisation) which relies on a Time-Stamp Token provided by the QV-TSA.

"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.

"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.

"Trust service" means an electronic service that enhances trust and confidence in electronic transactions.

"Trust Service Provider (TSP)" means an entity which provides one or more trust services.

"TSA Disclosure Statement" means an overview of the policies and practices of a TSA that require particular emphasis to subscribers and relying parties.

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

Additional definitions are provided in the CP/CPS.

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
TAV	Swiss Technical and Administrative Prescriptions for Certification Service Providers
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time
VZertES	Swiss Electronic Signature Ordinance
ZertES	Swiss Electronic Signature Law,

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. Refer to the "QuoVadis TSAs" section of the following QuoVadis web page for a list of QuoVadis TSUs https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx.

Below is a summary of the current QuoVadis TSUs and their issuers:

QuoVadis TSU Subject Distinguished Name	TSU Issuer	National Trust List relating to TSU Issuer
CN = eutsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.7 OU = Time-stamp Authority	QuoVadis EU Issuing Certification Authority G4	The Netherlands (https://www.acm.nl/en/tsl/)

QuoVadis TSU Subject Distinguished Name	TSU Issuer	National Trust List relating to TSU Issuer
O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL		
CN = eutsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.7 OU = Time-stamp Authority O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	QuoVadis EU Issuing Certification Authority G4	The Netherlands (https://www.acm.nl/en/tsl/)
CN = betsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.6 OU = Time-stamp Authority O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	QuoVadis Belgium Issuing CA G2	Belgium (https://tsl.belgium.be/)
CN = betsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.6 OU = Time-stamp Authority O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	QuoVadis Belgium Issuing CA G2	Belgium (https://tsl.belgium.be/)
CN = chtsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.1 OU = Time-stamp Authority O = QuoVadis Trustlink Schweiz AG 2.5.4.97 = NTRCH-CHE-112.210.349 C = CH	QuoVadis Swiss Regulated CA G1	N/A – Issued by a Swiss Issuing CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.
CN = chtsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.1 OU = Time-stamp Authority O = QuoVadis Trustlink Schweiz AG 2.5.4.97 = NTRCH-CHE-112.210.349 C = CH	QuoVadis Swiss Regulated CA G1	N/A – Issued by a Swiss Issuing CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.
CN = tsa02.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.3 OU = Thales TSS ESN:B87E-D107-917F	QuoVadis Root Certification Authority	N/A – Issued by a QuoVadis Root CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.

QuoVadis TSU Subject Distinguished Name	TSU Issuer	National Trust List relating to TSU Issuer
OU = Time-stamp Authority O = QuoVadis Limited C = CH		
CN = tsa01.quovadisglobal.com OU = 1.3.6.1.4.1.8024.0.2000.6.0 OU = nCipher DSE ESN:FBC9-3056-CE0A OU = Time-stamp Authority O = QuoVadis Limited C = CH	QuoVadis Root Certification Authority	N/A – Issued by a QuoVadis Root CA and Switzerland doesn't currently have a Trusted List. Audited under Swiss ZertES.

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. A Relying Party is an individual or entity relies on a TST generated a QuoVadis TSA. A Relying Party may or may not be a Subscriber. 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 EN 319 421. The private keys and the TSU meet the technical specifications of ETSI EN 319 422 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: http://www.quovadisglobal.com/repository.

5.2. IDENTIFICATION

The object-identifier (OID) of the QuoVadis Time-Stamping Policy is: 1.3.6.1.4.1.8024.0.2000.6.

This OID is referenced in every QuoVadis-issued time-stamp, and the QV-TSP/PS is available to both Subscribers and Relying Parties. Time-stamps bearing this OID are trusted in the Adobe Approved Trust List (AATL).

This QuoVadis Time-Stamping Policy is based on the ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1).

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.

QuoVadis 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)*. Refer to https://www.quovadisglobal.com/AboutUs/Accreditations.aspx for a list of QuoVadis´ audits and accreditations.

6. OBLIGATIONS AND LIABILITY

6.1. TSA OBLIGATIONS

6.1.1. 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 eIDAS, 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/PS and 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 that the private key used to sign the time-stamp token has not been compromised. Subscribers must use secure cryptographic functions for time-stamping requests. Subscribers must inform its end users (including any relevant Relying Parties) about the QV-TSP/PS, the CP/CPS. 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 revoked. 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 relevant QuoVadis CRL. QuoVadis CA Certificates, TSU Certificates and the related CRLS are published at https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx. 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 EN 319 421.

Note that QuoVadis has a number of different TSU Certificates, signed by different QuoVadis Issuing CAs. It is important that Relying Parties refer to https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx to determine the relevant TSU as this may also impact reliance.

ETSI EN 319 421 contains some additional requirements for Qualified electronic time-stamps as per the eIDAS Regulation. ETSI EN 319 421 states:

> *"The relying party is expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified."*

QuoVadis are currently operating under the transitional measures (Article 51) of the eIDAS Regulation. The public keys of the QuoVadis TSUs are not currently listed on any Trusted List. The issuers of some QuoVadis TSUs are listed on Trusted Lists. A summary of the QuoVadis TSUs, issuers and Trusted Lists is provided in section 4.2 "Time-stamping Authority".

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.

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:

- Contact information for QuoVadis and the QV-TSA is provided in section 1.5.2 (Contact Person) of the CP/CPS and also in the TSA Disclosure Statement.
- 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 EN 319 422 and TAV and are currently:
- Acceptable Time Stamp request Hashes: SHA-256, SHA-384, SHA-512
- Signature: sha256WithRSAEncryption (2048 bit key)
- The QuoVadis TSUs have a validity period of up to ten years.
- 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. If a trusted UTC time source can not be acquired the time stamp will not be issued.

- Use of the QuoVadis TSA may be limited to Certificate Holders of a valid QuoVadis Digital Certificate.
- 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 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.
- QuoVadis may charge fees for the services provided by the QuoVadis TSA.
- The applicable legal system and dispute resolution procedures relating to the QV-TSA are dealt with in the underlying Subscriber Agreement.
- TSA event logs are retained for 11 years in accordance with the retention period for audit logs in the CP/CPS.

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

QuoVadis TSU Public Keys are made available in a Digital Certificate. Refer to the "QuoVadis TSAs" section of the following QuoVadis web page for a list of QuoVadis TSUs https://www.quovadisglobal.com/QVRepository/DownloadRootsAndCRL.aspx. 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 information is provided in section 4.6 *Certificate Renewal* and section 4.7 *(Certificate ReKey)* of the CP/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.

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 in trusted roles, and the devices operate in a physically secured environment. Private keys are erased from modules when they are removed from service in according with the manufacturer's instructions. Additional information is provided in section 6.6 *(Life Cycle Technical Controls)* of the CP/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; and
- an identifier for the TSA and the TSU.

The QuoVadis TSUs maintain audit logs for all calibrations against the UTC(k) references.

7.3.2. Clock Synchronization with UTC

The QuoVadis TSA provides time with ±1 second of UTC by calibration with multiple independent time sources including GPS and National Measurement Institutes providing UTC(k) time.

The QuoVadis TSUs have technical measures in place to ensure that their time is synchronized with UTC within the declared accuracy. Audit and calibration records are maintained by QuoVadis. The QuoVadis TSA ensures that clock synchronisation is maintained when a leap second occurs as notified by the appropriate body.

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:
   - 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 operates from a resilient and secure hosting facility in accordance with the relevant provisions of ETSI EN 319 421.

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 EN 319 421. 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 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 EN 319 421. 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.