

# DigiCert Europe Time-Stamp Policy Practice Statement

Version 3.0, 7 November, 2025

# Table of Contents

|   |    |
|---|----|
| 1. SCOPE .....  | 4  |
| 2. REFERENCES .....   | 5  |
| 3. DEFINITIONS AND ABBREVIATIONS .....                      | 6  |
| 3.1. DEFINITIONS .....                                      | 6  |
| 3.2. ABBREVIATIONS .....                                    | 6  |
| 4. GENERAL CONCEPTS .....                                   | 8  |
| 4.1. GENERAL POLICY REQUIREMENTS CONCEPTS .....             | 8  |
| 4.2. TIME-STAMPING SERVICES .....                           | 8  |
| 4.3. TIME-STAMPING AUTHORITY .....                          | 8  |
| 4.3.1. Conformance .....                                    | 12 |
| 4.4. SUBSCRIBERS AND RELYING PARTIES .....                  | 12 |
| 4.5. TIME-STAMP POLICY AND AND TSA PRACTICE STATEMENT ..... | 13 |
| 5. TIME-STAMP POLICY .....                                  | 14 |
| 5.1. GENERAL .....  | 14 |
| 5.2. IDENTIFICATION .....                                   | 14 |
| 5.3. USER COMMUNITY AND APPLICABILITY .....                 | 14 |
| 6. POLICIES AND PRACTICES .....                             | 15 |
| 6.1. RISK ASSESSMENT .....                                  | 15 |
| 6.2. TRUST SERVICE PRACTICE STATEMENT .....                 | 15 |
| 6.2.1. Time-stamp Format .....                              | 15 |
| 6.2.2. Accuracy of the Time .....                           | 15 |
| 6.2.3. Limitations of the Service .....                     | 15 |
| 6.2.4. Obligations of the Subscriber .....                  | 16 |
| 6.2.5. Relying Party Obligations .....                      | 16 |
| 6.2.6. Verification of the Time-stamp .....                 | 16 |
| 6.2.7. Applicable Law .....                                 | 17 |
| 6.2.8. Availability .....                                   | 17 |
| 6.3. TERMS AND CONDITIONS .....                             | 17 |
| 6.4. INFORMATION SECURITY POLICY .....                      | 17 |
| 6.5. TSA OBLIGATIONS .....                                  | 18 |
| 6.5.1. General .....  | 18 |
| 6.5.2. TSA Obligations towards Subscribers .....            | 18 |
| 6.6. INFORMATION FOR RELYING PARTIES .....                  | 18 |
| 7. TSA MANAGEMENT AND OPERATION .....                       | 19 |
| 7.1. INTRODUCTION .....                                     | 19 |
| 7.2. INTERNAL ORGANISATION .....                            | 19 |
| 7.3. PERSONNEL SECURITY .....                               | 19 |
| 7.4. ASSET MANAGEMENT .....                                 | 19 |

|  |    |
|--|----|
| 7.5. ACCESS CONTROL .....  | 20 |
| 7.6. CRYPTOGRAPHIC CONTROLS .....                                | 20 |
| 7.6.1. General .....   | 20 |
| 7.6.2. TSU Key Generation .....                                  | 20 |
| 7.6.3. TSU Private Key Protection .....                          | 20 |
| 7.6.4. TSU Public Key Certificate .....                          | 20 |
| 7.6.5. Rekeying TSU's Key .....                                  | 21 |
| 7.6.6. Life Cycle Management of the Cryptographic Module .....   | 21 |
| 7.6.7. End of TSU Key Life Cycle .....                           | 21 |
| 7.7. TIME-STAMPING .....   | 21 |
| 7.7.1. Time-stamp Issuance .....                                 | 21 |
| 7.7.2. Clock Synchronisation with UTC .....                      | 21 |
| 7.8. PHYSICAL AND ENVIRONMENTAL SECURITY .....                   | 22 |
| 7.9. OPERATION SECURITY .....                                    | 22 |
| 7.10. NETWORK SECURITY .....                                     | 22 |
| 7.11. INCIDENT MANAGEMENT .....                                  | 23 |
| 7.12. COLLECTION OF EVIDENCE .....                               | 23 |
| 7.13. BUSINESS CONTINUITY MANAGEMENT .....                       | 23 |
| 7.14. TSA TERMINATION AND TERMINATION PLANS .....                | 24 |
| 7.15. COMPLIANCE .....   | 24 |
| 7.16 SUPPLY CHAIN .....  | 24 |
| 8. ADDITIONAL REQUIREMENTS FOR REGULATION (EU) NO 910/2014 ..... | 25 |

## Important Note About this Document

This is the Time-Stamp Policy/Practice Statement (DCEU-TSP/PS) of DigiCert Europe, a company of DigiCert, Inc. This DCEU-TSP/PS contains an overview of the policies, practices and procedures that DigiCert Europe employs for its operation as a Time-stamp Authority. This document is not intended to create contractual relationships between DigiCert Europe 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 DigiCert Europe and its business.

This document is controlled and managed under the authority of the DigiCert Policy Authority (DCPA). 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.

- Repository: <https://www.digicert.com/legal-repository/europe>
- Electronic mail: [policy@digicert.com](mailto:policy@digicert.com)
- Customer complaints email: [qvcomplaints@digicert.com](mailto:qvcomplaints@digicert.com)

### Locations

- **Belgium:** DigiCert Europe Belgium BV (previously QuoVadis Trustlink BVBA), Schaliënhoeverdreef 20T, 2800 Mechelen, Belgium. Phone: +32 15-79-65-21
- **Netherlands:** DigiCert Europe Netherlands B.V, Nevelgaarde 56 noord, 3436 ZZ Nieuwegein, The Netherlands. Phone: +31 (0) 30 232-4320
- **Switzerland:** DigiCert Switzerland AG, Poststrasse 17, Postfach, 9001 St. Gallen, Switzerland. Phone: +41 71-228-98-00

### 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       |

| <b>Author</b>   | <b>Date</b>             | <b>Versi<br/>on</b> | <b>Comment</b>   |
|-----------------|-------------------------|---------------------|--|
| QuoVadis<br>PMA | 19<br>November<br>2007  | 1.1                 | Updates to reflect trusted time source, new URL  |
| QuoVadis<br>PMA | 23 June 2008            | 2.0                 | Update to combine the Time-Stamp Policy and Practice Statement. Updates to reflect new URLs  |
| QuoVadis<br>PMA | 22 April<br>2010        | 2.1                 | Updates to algorithms  |
| QuoVadis<br>PMA | 11 October<br>2010      | 2.2                 | Updates to include more detail on validity period of TSA Certificate   |
| QuoVadis<br>PMA | 25 May 2012             | 2.3                 | Updates for trusted time source and supported algorithms   |
| QuoVadis<br>PMA | 25<br>November<br>2016  | 2.4                 | Updates for eIDAS, Regulation (EU) No 910/2014. Updates for ETSI EN 319 421 and ETSI EN 319 422  |
| QuoVadis<br>PMA | 2 June 2017             | 2.5                 | Updates for new Swiss TSA Certificates   |
| QuoVadis<br>PMA | 11 October<br>2019      | 2.6                 | Updates for new EU and Swiss TSA Certificates, Updates for accuracy  |
| QuoVadis<br>PMA | 20<br>November<br>2020  | 2.7                 | Editorial changes for alignment to ETSI EN 319 421, update to TSU information, change to QuoVadis Master Services Agreement/Subscriber Agreement |
| QuoVadis<br>PMA | 22 March<br>2021        | 2.8                 | Telephone change.  |
| QuoVadis<br>PMA | 17<br>September<br>2021 | 2.9                 | Minor updates to TSA table, time-stamp format, trusted roles, qcStatement reference.   |
| QuoVadis<br>PMA | 22<br>November<br>2021  | 2.10                | Updates to TSA table, validity period, RSA key size, CABF reference.   |
| QuoVadis<br>PMA | 1 August<br>2023        | 2.11                | Entity name updates. Incorporation of previous TSA Disclosure Statement into Section 6 of the current document. Update TSA certificates.         |
| QuoVadis<br>PMA | 11 August<br>2023       | 2.12                | Update TSA certificates.   |
| QuoVadis<br>PMA | 9 October<br>2023       | 2.13                | Minor correction to TSA certificate issuer name.   |
| DCPA            | 7 November<br>2025      | 3.0                 | Changes for compliance with ETSI updates; changes to company names, new TSA ICAs, and TSU Certificates. Updates to repository links.             |

## 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.

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 DigiCert Europe Time-stamping Authority (DCEU-TSA) uses Public Key Infrastructure and trusted time sources to provide reliable, standards-based Electronic Time-stamps. This DigiCert Europe Time-stamp Policy/Practice Statement (DCEU-TSPPS) defines the operational and management practices of the DCEU-TSA such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

The DCEU-TSA aims to deliver time-stamping services in accordance with the eIDAS regulation, as well as under other applicable national laws and regulations. However, DigiCert Europe Time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

Certain DigiCert Europe TSU provide Qualified Electronic Time-stamps under eIDAS and other national laws or regulations; see Section 4.3 (Time-stamping Authority) of this document.

## 2. REFERENCES

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

1. 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)
2. ETSI EN 319 401: Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
3. ETSI EN 319 411-1: Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements
4. ETSI EN 319 411-2: Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
5. ETSI EN 319 412-3: Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
6. ETSI EN 319 412-5: Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
7. ETSI EN 319 421: Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
8. ETSI EN 319 422: Electronic Signatures and Trust Infrastructures (ESI); Time-stamping Protocol and Time-stamp Token Profiles
9. ETSI TS 119 312: Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites
10. DigiCert Europe Certificate Policy/Certification Practice Statement (CP/CPS)
11. RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)
12. SR 943.03 (ZertES), Switzerland, Electronic Signature Law; SR 943.032 (VZertES), Switzerland, Swiss Electronic Signature Ordinance; and 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. CA/Browser Forum Baseline Requirements for Code Signing Certificates



## 3. DEFINITIONS AND ABBREVIATIONS

### 3.1. DEFINITIONS

**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.

**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 issued by a Qualified TSP and whose TSU Public Key Certificate was issued by a CA operating under a ETSI EN 319 411-2 certificate policy.

**Relying party** means an entity (an individual or organisation) which relies on a Time-stamp Token provided by the DCEU-TSA.

**Subscriber** means an entity (an individual or organisation) which requires the services provided by a TSA and has entered into the relevant agreement with DigiCert Europe.

**Time-stamping Authority or TSA** means a trusted authority which issues Time-stamps.

**Time-stamp** means a data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.

**Time-stamping 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 Provider** means an entity which provides one or more electronic service that enhances trust and confidence in electronic transactions.

**UTC(k)** means a time scale realised by a laboratory “k” as defined in Bureau International des Poids et Mesures (BIPM) Circular T.

Additional definitions are provided in the CP/CPS.

### 3.2. ABBREVIATIONS

**CP/CPS** Certificate Policy/ Certification Practice Statement

**CRL** Certificate Revocation List

**ETSI** European Telecommunications Standards Institute

**HSM** Hardware Security Module

**PKI** Public Key Infrastructure

**TSP** Trust Service Provider



## 4. GENERAL CONCEPTS

### 4.1. GENERAL POLICY REQUIREMENTS CONCEPTS

The present document references ETSI EN 319 401 General Policy Requirements for Trust Service Providers for generic policy requirements common to all classes of TSP services.

The structure and contents of this DCEU-TSP/PS are laid out in accordance with ETSI EN 319 421, Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing TimeStamps.

The DCEU-TSP/PS is administered and approved by the DigiCert Policy Authority (DCPA), and should be read in conjunction with the relevant DigiCert Europe CP/CPS.

### 4.2. TIME-STAMPING SERVICES

Time-stamping services include the following components:

- Time-stamping provision: the technical component that issues the Time-stamps; and
- Time-stamping management: the service component that monitors and controls the time-stamping operation, including synchronisation with the reference UTC time source, according to the DCEU-TSP/PS.

QuoVadis adheres to the international standards in Section 2 (References) of this document to increase the trustworthiness of the time-stamping services.

### 4.3. TIME-STAMPING AUTHORITY

A Time-stamping Authority (TSA) is a TSP trusted by the users (i.e., Subscribers as well as Relying Parties) to issue secure Time-stamps as described in RFC 3161. The DCEU-TSA takes overall responsibility for the provision of time-stamping services identified in Section 4.2 (Time-stamping Services) of this document. DigiCert Europe operates the DCEU-TSA as part of its PKI.

The DCEU-TSA has responsibility for the operation of one or more Time-stamping Units (TSU) which create and sign Time-stamps on behalf of the TSA. Each TSU has a different key. Refer to the DigiCert Europe TSAs” section of <https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates> for a complete list of DigiCert Europe TSUs.

Following is a summary of the current DigiCert Europe TSUs and their issuers. Qualified TSAs do not provide Timestamp Tokens to the public until the TSU Public Key Certificates are listed on a relevant audit and/or Trusted List.

| Status  | Key | Identifiers   |
|---|-----|---|
| eIDAS - Netherlands<br>Qualified Electronic Time-stamp<br><a href="https://webgate.ec.europa.eu/tlbrowser/#/tl/NL/9/14">https://webgate.ec.europa.eu/tlbrowser/#/tl/NL/9/14</a><br>Time-stamp Tokens may contain the “esi4-qtstStatement-1” extension | RSA | Issuer: DigiCert QuoVadis G3 TS Europe<br>RSA4096 SHA256 2023 CA1<br>CN = tsaeursa1.digicert.eu<br>CN = tsaeursa2.digicert.eu<br>CN = tsaeursa3.digicert.eu<br><br>O = QuoVadis Trustlink B.V.<br>Org Identifier= NTRNL-30237459<br>C = NL<br>-<br><br>Issuer: DigiCert QV G3 TS EUR RSA4096<br>RSASSA-PSS 2025 CA1<br><br>Issuer: DigiCert QV G3 TS Europe RSA4096<br>SHA256 2025 CA1<br>CN= tsaeu2025rsa1.digicert.eu<br>CN = tsaeu2025rsa2.digicert.eu<br>CN = tsaeu2025rsa3.digicert.eu<br><br>O = DigiCert Europe Netherlands B.V.<br>Org Identifier= NTRNL-30237459<br>C = NL |

| Status  | Key       | Identifiers  |
|---|-----------|--|
| eIDAS - Netherlands<br>Qualified Electronic Time-stamp<br><a href="https://webgate.ec.europa.eu/tlbrowser/#/tl/NL/9/14">https://webgate.ec.europa.eu/tlbrowser/#/tl/NL/9/14</a><br>Time-stamp Tokens may contain the “esi4-qtstStatement-1” extension | ECD<br>SA | Issuer: QuoVadis Time-Stamping Authority CA G2<br><br>CN = tsaeuecc1.quovadisglobal.com<br>CN = tsaeuecc2.quovadisglobal.com<br>CN = tsaeuecc3.quovadisglobal.com<br><br>O = QuoVadis Trustlink B.V.<br>Org Identifier= NTRNL-30237459<br>C = NL<br>-<br><br>Issuer: DigiCert QuoVadis G3 TS Europe ECC P256 SHA256 2023 CA1<br>CN = tsaeuecc1.digicert.eu<br>CN = tsaeuecc2.digicert.eu<br>CN = tsaeuecc3.digicert.eu<br><br>O = QuoVadis Trustlink B.V.<br>Org Identifier= NTRNL-30237459<br>C = NL<br>- Issuer: CN = DigiCert QV G3 TS Europe ECC P256 SHA256 2025 CA1<br>CN = tsaeu2025ecc1.digicert.eu<br>CN = tsaeu2025ecc2.digicert.eu<br>CN = tsaeu2025ecc3.digicert.eu<br><br>O = DigiCert Europe Netherlands B.V.<br>ON = NTRNL-30237459<br>C = NL |
| Belgium TSA not featured on a Trusted List  | ECD<br>SA | Issuer: QuoVadis Time-Stamping Authority CA G2<br><br>CN = tsabeecc1.quovadisglobal.com<br>CN = tsabeecc2.quovadisglobal.com<br>CN = tsabeecc3.quovadisglobal.com<br><br>O = DigiCert Europe Belgium B.V.<br>Org Identifier = NTRBE-0537698318<br>C = BE   |

| Status  | Key | Identifiers  |
|---|-----|--|
| ZertES – Switzerland Qualified Electronic Time-stamp Time-stamp Tokens may contain the “esi4-qtstStatement-1” extension | RSA | <p>Issuer: QuoVadis Time-Stamping Authority CA G1</p> <p>CN = tsachrsa1.quovadisglobal.com<br/> CN = tsachrsa2.quovadisglobal.com<br/> CN = tsachrsa3.quovadisglobal.com</p> <p>O = QuoVadis Trustlink Schweiz AG<br/> Org Identifier = NTRCH-CHE-112.210.349<br/> C = CH<br/> -</p> <p>Issuer: DigiCert QuoVadis G3 TS Europe RSA4096 SHA256 2023 CA1</p> <p>CN = tsachrsa1.digicert.eu<br/> CN = tsachrsa2.digicert.eu<br/> CN = tsachrsa3.digicert.eu</p> <p>O = QuoVadis Trustlink Schweiz AG<br/> 2.5.4.97 = NTRCH-CHE-112.210.349<br/> C = CH</p> <p>Issuer: DigiCert QV G3 TS Switzerland RSA4096 SHA256 2025 CA1<br/> Issuer: DigiCert QV G3 TS Switzerland RSA4096 RSASSA-PSS 2025 CA1<br/> O = DigiCert Switzerland AG<br/> Org Identifier = NTRCH-CHE-112.210.349<br/> C = CH</p> |

| Status   | Key       | Identifiers  |
|--|-----------|--|
| ZertES – Switzerland Qualified Electronic Time-stamp<br>Time-stamp Tokens may contain the “esi4-qtstStatement-1” extension | ECD<br>SA | <p>Issuer: QuoVadis Time-Stamping Authority CA G2</p> <p>CN = tsachecc1.quovadisglobal.com<br/>CN = tsachecc2.quovadisglobal.com<br/>CN = tsachecc2.quovadisglobal.com</p> <p>O = QuoVadis Trustlink Schweiz AG<br/>Org Identifier = NTRCH-CHE-112.210.349<br/>C = CH<br/>-</p> <p>Issuer: DigiCert QuoVadis G3 TS Switzerland ECC P256 SHA256 2023 CA1</p> <p>CN = tsachecc1.digicert.eu<br/>CN = tsachecc2.digicert.eu<br/>CN = tsachecc3.digicert.eu</p> <p>O = QuoVadis Trustlink Schweiz AG<br/>2.5.4.97 = NTRCH-CHE-112.210.349<br/>C = CH</p> |

### 4.3.1. Conformance

DigiCert Europe references the policy identifier in Section 5.2 (Identification) of this document in all Time-stamps to indicate conformance with this policy. DigiCert Europe is subject to periodic independent internal and external reviews to demonstrate that the DCEU-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.digicert.com/webtrust-audits> for a list of DigiCert Europe’s audits and accreditations.

Where aspects of the DCEU-TSA are Qualified, DigiCert Europe confirms that the DCEU-TSA is audited annually by a Conformity Assessment Body, and the assessment report is submitted to the relevant national Supervisory Body. Where the Supervisory Body requires DigiCert Europe to remedy any failure to fulfil requirements, DigiCert Europe will act accordingly and in a timely fashion. The Supervisory Body will be informed of any change in the provision of the relevant DCEU-TSA.

## 4.4. SUBSCRIBERS AND RELYING PARTIES

Subscribers are entities that hold a service contract with DigiCert Europe and have agreed to the DigiCert Europe Timestamping Authority Subscriber Agreement. A Relying Party is an individual or entity relies on a Time-stamp generated a DigiCert Europe 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 DCEU-TSP PS.

## **4.5. TIME-STAMP POLICY AND AND TSA PRACTICE STATEMENT**

This DCEU-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.

Additional internal documents define how DigiCert Europe meets the technical, organisational, and procedural requirements identified in the DCEU-TSP/PS. These documents may be provided only under strictly controlled conditions. All DigiCert Europe policies and practices are under the control of the DCPA.

This DCEU-TSP/PS extends the CP/CPS which regulates the operation of the DCEU-PKI and associated Trust Services. The DCEU-TSP/PS and CP/CPS are public documents and may be downloaded at <https://www.digicert.com/legal-repository/europe>



# 5. TIME-STAMP POLICY

## 5.1. GENERAL

This TSP defines a set of processes for the trustworthy creation of Time-stamps 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 DCEU-TSA signs Time-stamps using Private Keys that are reserved specifically for that purpose. Each Timestamp contains an identifier to the applicable policy, and Time-stamps are issued with time accurate to  $\pm 1$  second or better 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.

## 5.2. IDENTIFICATION

The DCEU-TSP/PS defines a time-stamp policy identified by OID 1.3.6.1.4.1.8024.0.2000.6 and aligns to the Baseline Time-Stamp Policy (BTSP) in ETSI EN 319 421 (OID 0.4.0.2023.1.1). Any deviations from the BTSP are explicitly stated in this document.

## 5.3. USER COMMUNITY AND APPLICABILITY

The user community for DigiCert Europe Time-stamps includes only Subscribers and their Relying Parties. All Subscribers are automatically deemed to be Relying Parties. DigiCert Europe does not provide public Time-stamp services.

DigiCert Europe 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. DigiCert Europe Time-stamps may be applied to any application requiring proof that a datum existed before a particular time.

# 6. POLICIES AND PRACTICES

## 6.1. RISK ASSESSMENT

DigiCert Europe performs annual risk assessments aligned with ETSI EN 319 401, Section 5 that identify and assess reasonably foreseeable internal and external threats to the DigiCert Europe PKI, including the DCEU-TSA service. Based on the risk assessment, DigiCert Europe develops, implements, and maintains a security plan to manage and control the risks identified during the risk assessment. See Section 5.4.8. (Vulnerability Assessment) of the CP/CPS.

## 6.2. TRUST SERVICE PRACTICE STATEMENT

DigiCert Europe operates the DCEU-TSA and assumes responsibility that the requirements of Section 7 (TSA Management and Operation) of this document - as well as the provisions of eIDAS, ZertES and the TAV regulations, and the ETA - are implemented as applicable to the selected trusted Time-stamp policy.

The DCEU-TSP/PS is administered and approved by the DCPA. DigiCert Europe is a party to the mutual agreements and obligations between the DCEU-TSA, Subscribers, and Relying Parties. The DCEU-TSP/PS and CP/CPS are integral components of these agreements.

### 6.2.1. Time-stamp Format

DigiCert Europe Time-stamps are compliant with RFC 3161 (including support for reqPolicy, nonce, and certReq). The cryptographic algorithms and key lengths used by the DCEU-TSA comply with ETSI EN 319 422 and TAV:

- Acceptable Time-stamp request hashes: SHA-256, SHA-384, SHA-512
- Signature: sha256WithRSAEncryption (minimum 3072 bit key) or sha256WithECDSA (p-256 key)

TSU Public Key Certificates using RSA may have a validity period no longer than three years and using ECDSA may have a validity period no longer than six years. The DCPA conducts periodic reviews to determine if algorithms or key sizes used within the DigiCert Europe PKI are vulnerable.

### 6.2.2. Accuracy of the Time

The DCEU-TSA provides time within  $\pm 1$  second or better of UTC. A time signal is provided to the TSUs from GNSS which is GPS traceable to UTC via USNO, as well as from three independent Stratum-1 time sources located in Switzerland and Germany.

The time included in a Time-stamp is the time of processing by the TSU, not the time of submission nor of acceptance.

### 6.2.3. Limitations of the Service

No stipulation.

## 6.2.4. Obligations of the Subscriber

Subscribers must verify that the Time-stamp has been correctly signed and check that the Private Key used to sign the Time-stamp has not been compromised. Subscribers must use secure cryptographic functions for time-stamping requests. Subscribers must inform end users (including any relevant Relying Parties) about the DCEU-TSP/PS, the CP/CPS. Subscriber obligations are also defined in the relevant DigiCert Europe Agreements (including the Master Services Agreement, Subscriber Agreement, Terms of Use, and Relying Party Agreement as applicable).

## 6.2.5. Relying Party Obligations

Before placing any reliance on a time-stamp, Relying Parties must verify that the Time-stamp has been correctly signed and that the Private Key used to sign the Time-stamp has not been revoked. The Relying Party should take into account any limitations on usage of the Time-stamp indicated by this DCEU-TSP/PS and any other reasonable precautions. During the TSU Certificate validity period, the status of the Private Key can be checked using the relevant Certificate Status service (which includes CRL or OCSP). DigiCert Europe CA and TSU Certificates are published at <https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates>.

Note that DigiCert Europe operates multiple TSU, signed by different DigiCert Europe Issuing CAs. Specific TSU Certificates may be listed on Trusted Lists. See Section 4.3 (Time-stamping Authority) of this document to determine the relevant TSU and its status.

ETSI EN 319 421 contains some additional requirements for Qualified Electronic Time-stamps in accordance with the eIDAS Regulation. See Section 8 (Additional Requirements) of this document.

### 6.2.5.1. Long term Verification of Time-stamps

In line with Annex D of ETSI EN 319 421, verification of a Time-stamp can still be performed after the end of the validity period of the Certificate, if at the time of verification:

- the TSU Private Key has not been compromised;
- the hash algorithm, signature algorithm and signature key size are still supported by this DCEU-TSP/PS.

Technical developments can reduce the security value of Time-stamped data. Validity may be maintained by applying an additional Time-stamp to protect the integrity of the previous one. Alternatively, the Time-stamped data may be placed in secure storage.

## 6.2.6. Verification of the Time-stamp

Time-stamp verification includes the following steps:

- Verification of the Time-stamp issuer. See also Section 4.3 (Time-stamping Authority) of this document; and
- Verification of the revocation status of the Certificates in the Time-stamp.

### **6.2.7. Applicable Law**

Any controversy or claim relating to the DCEU-TSA shall be addressed according to Section 9.13 (Dispute Resolution Procedures) and Section 9.13 (Governing Law) of the CP/CPS.

### **6.2.8. Availability**

DigiCert Europe has implemented measures to enable 24x7 operation of the DCEU-TSA. Although those measures provide high service availability, DigiCert Europe does not guarantee an annual availability of 100%.

Use of the DCEU-TSA may be limited to Holders of a valid DigiCert Europe Certificate. DigiCert Europe may charge fees for the services provided by the DCEU-TSA.

## **6.3. TERMS AND CONDITIONS**

Key terms governing DigiCert Europe's time-stamping services—including service scope, permitted and prohibited uses, service availability objectives, and liability limitations—are defined in the applicable DigiCert Europe Agreements (Master Services Agreement, Terms of Use, and/or other applicable contractual terms).

## **6.4. INFORMATION SECURITY POLICY**

DigiCert Europe has a formal Information Security Policy that documents the DigiCert Europe policies, standards, and guidelines relating to information security. This Information Security Policy has been approved by DCPA and is communicated to all employees.

## **6.5. TSA OBLIGATIONS**

### **6.5.1. General**

No stipulation.

### **6.5.2. TSA Obligations towards Subscribers**

DigiCert Europe undertakes the following obligations to DCEU-TSA Subscribers:

- To operate in accordance with this DCEU-TSP/PS and the CP/CPS;
- To ensure that TSUs maintain a minimum UTC time accuracy of  $\pm 1$  second or better;
- Undergo internal and external reviews to assure compliance with relevant legislation and DigiCert Europe policies and procedures; and
- To provide high availability access to DCEU-TSA systems except in the case of planned technical interruptions, loss of time synchronization, or Certificate verification issues.

## **6.6. INFORMATION FOR RELYING PARTIES**

When relying upon a Time-stamp, Relying Parties have an obligation to verify that the Time-stamp has been correctly signed and that the Private Key used to sign the Time-stamp has not been compromised until the time of the verification. See also Section 6.2.5 (Relying Party Obligations) and 6.2.6 (Verification of the Timestamp) of this document.

# 7. TSA MANAGEMENT AND OPERATION

## 7.1. INTRODUCTION

DigiCert Europe has implemented information security policies and operational procedures to maintain the security of the DCEU-TSA service.

## 7.2. INTERNAL ORGANISATION

The DCEU-TSA is operated by DigiCert Europe and affiliated companies. Information security and quality management of the DCEU-TSA is carried out within the security concept of the service. DigiCert Europe PKI services are provided from datacentres located in the Netherlands and Switzerland.

## 7.3. PERSONNEL SECURITY

To enhance the trustworthiness of its PKI operations, DigiCert Europe maintains appropriate personnel practices fulfilling security best practice and the requirements of relevant standards such as Section 7.2 of ETSI EN 319 401. Additional information is provided in Section 5.2 (Procedural Controls) and Section 5.3 (Personnel Controls) of the CP/CPS.

In particular:

1. DigiCert Europe employs personnel whom possess the expert knowledge, experience and qualifications and who have received training regarding security and data protection as appropriate for the offered services and the job function.
2. Trusted roles, on which the security of the DCEU-TSA is dependent, are clearly identified in the CP/CPS.
3. Security roles and responsibilities are documented in 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.
4. Personnel shall exercise administrative and management procedures and processes that are in line with the Information Security Policy.

## 7.4. ASSET MANAGEMENT

In order to ensure that information and other assets receive appropriate security treatment, DigiCert Europe maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis and the requirements of relevant standards such as Section 7.3 of ETSI EN 319 401. Additional information is provided in Section 6.6 (Life Cycle Technical Controls) of the CP/CPS.

## 7.5. ACCESS CONTROL

Operational access to the DCEU-TSA system is limited to authorised individuals through practices aligned with relevant standards such as Section 7.3 of ETSI EN 319 401. Additional information is provided in Section 5.2 (Procedural Controls), Section 5.3 (Personnel Controls), and Section 6.7 (Network Security Controls) of the CP/CPS.

## 7.6. CRYPTOGRAPHIC CONTROLS

### 7.6.1. General

Practices of the DCEU-TSA for cryptographic controls are aligned with Section 7.5 of ETSI EN 319 401. Several DigiCert Europe Private Keys are used to deliver the DCEU-TSA service: a DigiCert Europe Issuing CA is used to issue the Time-stamp Certificates which are used within the TSUs to issue Time-stamps.

### 7.6.2. TSU Key Generation

DigiCert Europe generates the cryptographic keys used in its DCEU-TSA services under M of N control by authorised personnel acting in trusted roles in a secure physical environment. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. Additional information is provided in Section 5.2.1 (Trusted Roles) and 6.1 (Key Generation and Installation) of the CP/CPS.

The keys are generated within TSU HSMs that are certified to at least FIPS 140-2 Level 3 or higher. Permitted algorithms and key size are described in Section 6.2.1 (Time-stamp Format) of this document.

### 7.6.3. 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 at least FIPS 140-2 Level 3 or higher to hold and sign with the keys.

Upon creation of new TSU Private Keys, they are backed up. Backups are copied, stored, and recovered only by personnel in trusted roles under M of N control in a physically secured environment. Any backup copies of the TSU signing Private Keys are stored in an encrypted form.

### 7.6.4. TSU Public Key Certificate

DigiCert Europe TSU Public Keys are made available in a Public Key Certificate. Refer to the “Quovadis brand root CA certificates” section of the Download CAs area of <https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates>. The TSU do not issue Time-stamps before the corresponding Public Key Certificate is loaded into the TSU or its cryptographic device.

### **7.6.5. Rekeying TSU's Key**

TSU signing Private Keys shall be replaced if the DCPA determines that the algorithm or key size is vulnerable or unsuitable (see Section 7.6.1 of this document). Additional information is provided in Section 4.6 (Certificate Renewal) and Section 4.7 (Certificate Re-Key) of the CP/CPS.

### **7.6.6. Life Cycle Management of the Cryptographic Module**

DigiCert Europe has in place procedures to ensure that HSMs 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 accordance with the manufacturer's instructions. Additional information is provided in Section 6.2 (Private Key Protection and Cryptographic Module Engineering Controls) of the CP/CPS.

### **7.6.7. End of TSU Key Life Cycle**

TSU Private Keys are replaced before the notAfter date of their associated Public Key Certificate. TSU Private Keys are not used beyond their expiration date. The TSU rejects any attempt to issue Time-stamps once a Private Key has expired. After expiration, the Private Keys are destroyed in a manner such that the Private Keys cannot subsequently be retrieved or used.

## **7.7. TIME-STAMPING**

### **7.7.1. Time-stamp Issuance**

Time-stamps conform with the profile as defined in ETSI EN 319 422. Time-stamps are issued securely and include the correct time. The provision of a Time-stamp in response to a request is at the discretion of DigiCert Europe.

### **7.7.2. Clock Synchronisation with UTC**

The DCEU-TSA provides time within  $\pm 1$  second or better of UTC. A time signal is provided to the TSUs which is GPS time traceable to UTC via USNO, as well as from three independent Stratum-1 time sources located in Switzerland and Germany.

The DCEU-TSA ensures that clock synchronisation is maintained when a leap second occurs as notified by the International Earth Rotation and Reference Systems Service (IERS) or other appropriate body.

TSU clocks are protected within the HSMs and are recalibrated hourly 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 DCEU-TSA does not issue Time-stamps until correct time is restored. Manual administration of the TSU clock requires M of N authorised personnel. Audit and calibration records are maintained by the DCEU-TSA.



## 7.8. PHYSICAL AND ENVIRONMENTAL SECURITY

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

1. Access controls are applied to the cryptographic modules to meet the requirements of Section 7.6 (Cryptographic Controls).
2. 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 unauthorised access to systems or data.
  - Every entry to the physically secure area is subject to independent oversight and non-authorised person shall be accompanied by an authorised person whilst in the secure area. Every entry and exit is logged.
  - 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 organisations 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 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 authorisation.

See also Section 5.1 (Physical Controls) of the CP/CPS.

## 7.9. OPERATION SECURITY

DigiCert Europe has an active security management programme designed to document, implement, and maintain adequate security provisions for the DCEU-PKI according to best practice and the requirements of relevant standards. The DCPA is the body responsible for setting policies and practices for the overall PKI including the 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.

## 7.10. NETWORK SECURITY

DigiCert Europe maintain and protect all TSU systems in a secure zone which may only be accessed by personnel with trusted roles. TSU systems by are configured to remove or disable accounts, applications, services, protocols, and ports that are not used in the DCEU-TSA operations. Additional information is provided in Section 6 (Technical Security Controls) of the CP/CPS.

## 7.11. INCIDENT MANAGEMENT

DigiCert Europe maintains internal incident response procedures aligned with ETSI EN 319 401, Section 7.9 to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. DigiCert Europe reviews, tests, and updates its incident response plans and procedures on a periodic basis.

These procedures include notification to appropriate Conformance Assessment Bodies and Supervisory Authorities in the event of a disaster, security compromise, loss of time synchronisation, or business failure. Information will be provided to contracted Subscribers and Relying Parties and posted on a DigiCert Europe website. Additional information is provided in Section 5.7 (Compromise and Disaster Recovery) of the CP/CPS.

## 7.12. COLLECTION OF EVIDENCE

DigiCert Europe maintains records of relevant information concerning the operation of the DCEU-TSA for a period of 11 years. Additional information is provided in Section 5.4 (Audit Logging Procedures) of the CP/CPS.

Records include:

- Events relating to the life-cycle of TSU keys and Certificates; and
- Events related to clock re-calibration and synchronisation.

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 but may be provided at the request of Subscribers or if required by court order or other legal requirement.

## 7.13. BUSINESS CONTINUITY MANAGEMENT

In the event of compromise of a TSU Private Key, DigiCert Europe 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 DigiCert Europe Certificate Status service. 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. The DCEU-TSA maintains audit trails to discriminate between genuine and backdated tokens.

In the event of a compromise, or suspected compromise of a Private Key, or loss of calibration when issuing time-stamps, DigiCert Europe will notify, as appropriate Conformance Assessment Parties and Supervisory Authorities, and make best efforts to provide Subscribers and Relying Parties with information to identify the Time-stamps which may have been affected, unless this breaches the privacy of the DCEU-TSA users or the security of the DCEU-TSA services.

## **7.14. TSA TERMINATION AND TERMINATION PLANS**

In the case of termination of the DCEU-TSA, DigiCert Europe will follow the procedures in Section 5.8 (Certificate Authority and/or Registration Authority Termination) of the CP/CPS and also more detailed internal DigiCert Europe termination procedures. These include at a minimum informing relevant Supervisory Authorities and Subscribers and transferring obligations to a reliable party for maintaining event log and audit archives. TSU Certificates will be revoked or TSU Private Keys destroyed. When the TSA terminates its services, the TSUs shall not issue new Time-stamp Tokens.

## **7.15. COMPLIANCE**

The DCEU-TSA complies with applicable regulations and legal requirements (including eIDAS and ZertES), as well as the requirements of the DigiCert Europe Privacy Policy (see <https://privacy.digicert.com/>).

## **7.16 SUPPLY CHAIN**

DigiCert Europe implements processes and procedures to address security risks associated with the use of products and services provided by suppliers to the DCEU-TSA.

## 8. ADDITIONAL REQUIREMENTS FOR REGULATION (EU) NO 910/2014

When a Time-stamp is claimed to be a Qualified Electronic Time-stamp as per Regulation (EU) No 910/2014, the TSU or TSA ICA Public Key Certificate will be listed on an EU Trusted List, will be issued in compliance with the NCP+ certificate policy as specified in ETSI EN 319 411-1, and with ETSI EN 319 411-2. The Time-stamp response may contain the qcStatement "esi4-qtstStatement-1" as defined in ETSI EN 319 422.

A Relying Party is expected to use a Trusted List to establish whether the TSP and the TSA ICA or TSU are Qualified. If the Public Key of the TSU is listed in the Trusted List and the TSP it represents is a Qualified time-stamping service, then the Time-stamps issued by this TSU can be considered as Qualified.