DigiStamp
Time-Stamping Authority
Policy and Practice

Version: 3.1

Published: December 31, 2014

Table of Contents

Introduction

In creating reliable and manageable digital evidence, it becomes necessary to have an agreed-upon method of associating data with a point-in-time, in manner that can be recognized as valid long into the future. The process and the resulting data structures determine the quality of the digital evidence to anchor events, by time, in the real world.

Generically, the value of digital content of all types is enhanced when it can be proven when that content existed.

A common transaction is a digitally signed document, where it is necessary to prove that the digital signature from the signer was applied when the signer's certificate was valid.

To prove the digital signature was generated while the signer's certificate was valid, the digital signature must be verified and the following conditions satisfied:

1. The validity period of the signer's certificate must include the time of verification; and the signer's certificate must not have been revoked.

2. Or, it must be provable that the signature was created within the signer's certificate's validity period and before revocation occurred.

The trusted digital time-stamp has value in the business sector and is an important component of electronic signatures, also featured by the ETSI Electronic Signature Format standard TS 101 733, built upon the Time-Stamp protocol from the IETF (RFC 3161). Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term electronic signatures.

The Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures defines certification-service-provider as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures". One example of a certification- service-provider is a time-stamping authority.

DigiStamp applies to and abides by the Time-Stamp protocol from the IETF (RFC 3161), with the exception of the FIFO directive; DigiStamp has implemented a queueing and quality-of-service wrapper for TSA services. DigiStamp maintains a Long Term Archive of Timestamps that abides by the Evidence Record Syntax and processing rules from the IETF (RFC 6283). This document serves to communicate to the public the nature of the policy and methods of practice that DigiStamp has implemented as a Time-Stamping Authority.

The structure and content[1] of this TSA Policy and Practice Statement are compatible with IETF RFC 3628 and the associated ETSI TS 102 023.

[1] Portions of this document and outline are derived from RFC 3628 that retains a copyright by The Internet Society. See the full copyright notice at the end of this document.

DigiStamp

DigiStamp, Inc is incorporated in Delaware with its principle place of business in Texas and shall be governed by the laws of the state of Texas (USA) without regard to conflict of laws principles and without regard to the 1980 United Nations Convention on the International Sale of Goods. DigiStamp time-stamps meets the time-stamping requirements set forth by RFC 3161. DigiStamp waives all liability for the delivery of TSTs.

The authority of DigiStamp timestamps is ensured by the entire no-export signing key lifecycle, and trusted timekeeping, occurring inside a FIPS 140 Level 3+ HSM which was locked down in an audited event to be un-upgradeable from code signed in an audited event. SecureTime® means no one can falsify a timestamp or tamper with a trusted system, not even DigiStamp.

DigiStamp takes very seriously our responsibility to meet the claims set forth in our Terms and Conditions, including the availability and accuracy of time-stamping services. DigiStamp guarantees subscribers their constant access to DigiStamp TSA services. Since inception of service in 2001, availability of service without exception or break has been 99.99%. Disaster Recovery and Business Continuity Plans have been drafted and tested to ensure continuation of service during unforeseen circumstances. Redundant, geographically separated servers are used to ensure continual access to DigiStamp's service. You select one of the DigiStamp server locations; however, in the event the selected server is temporarily unavailable, the client software can automatically failover to another server. DigiStamp continually monitors server utilization to ensure availability and response time.

DigiStamp also takes very seriously our commitment to protecting the privacy of users of our services. For more information on our practices regarding your privacy, please visit www.digistamp.com/about-us/privacy-and-legal-policies/.

The users of DigiStamp time stamp service agree to the terms and conditions of the End User License Agreement (EULA). For more information on available warranties, see "Article IV. Warranty, Warranty Disclaimers and Limitations on Liability". For more information on applicable laws and complaint/dispute resolution, note Section 3.09 *Governing Law*, Section 3.10 *Jurisdiction / Venue*, Section 3.11 *Arbitration*, and Section 3.12 *Unicitral Exclusion*.

DigiStamp complies with a number of industry standards covering many topics, including:

1) IETF RFC 2459
2) IETF RFC 2630
3) IETF RFC 3126
4) IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)"
5) IETF RFC 3161 Besides this, other data structures and protocols may also be appropriate, such as defined in ISO-18014-1.2002, ISO-18014-2.2002, ISO-18014-3.2004, and ANSI.X9-95.2005
6) IETF RFC 3628 and the associated ETSI TS 102 023
7) NIST FIPS PUB 180
8) Uniform Rules of Evidence Code
9) Uniform Electronic Transactions Act
10) 18 U.S.C. 1343 Wire Fraud
11) 18 U.S.C. 2701 Electronic Communications Privacy Act
12) 18 U.S.C. 2510 regarding electronic communications
13) 18 U.S.C. 1028 Fraud & related activity in connection with identification documents and information

When we compile, install, and initialize our servers, we use two professional, qualified, external auditors. In a rigorous multi-hour process, these independent professionals witness the initialization and lock-down of the TSA HSM. The TSA HSM is the trusted third-party witnessing your data with its specially-customized hardware. The IBM 4758 or 4765 Coprocessor is certified at levels 3 or superior of the rigorous National Institute of Standards and Technology (NIST) using the Security Requirements for Cryptographic Modules.
For additional information, please visit: www.digistamp.com

1 Scope

The present document specifies policy requirements relating to the operation of DigiStamp as a Time-stamping Authority (TSA). The present document defines policy requirements on the operation and management practices of DigiStamp such that subscribers and relying parties may have confidence in the operation of the time-stamping services.

These policy requirements may be applied to any application requiring proof that a datum existed before a particular time. This policy supports the specific requirement of time-stamping services used in support of qualified electronic signatures (i.e. in line with article 5.1 of the European Directive on a community framework for electronic signatures).

These policy requirements are based upon the use of public key cryptography, public key certificates, cryptographic hash algorithms, long-term archiving, hash tree chaining and reliable time sources.

Independent bodies may use the present document as the basis for confirming that DigiStamp may be trusted for providing time-stamping services.

The current document addresses requirements for DigiStamp issuing time-stamp tokens which are synchronized with Coordinated universal time (UTC) and digitally signed by DigiStamp.

Subscriber and relying parties should consult DigiStamp's practice statement (Section 7 of this document) to obtain further details of precisely how this time-stamp policy is implemented by DigiStamp (e.g. protocols used in providing this service).

The current document does not specify:

- protocols used to access DigiStamp;
- how the requirements identified herein may be assessed by an independent body;
- requirements for information to be made available to such independent bodies;
- requirements on such independent bodies

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

1. ITU-R Recommendation TF.460-5 (1997): "Standard-frequency and time-signal emissions".
2. ITU-R Recommendation TF.536-1 (1998): "Time-scale notations".
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
4. FIPS PUB 140-1 (1994): "Security Requirements for Cryptographic Modules".
5. ISO/IEC 15408 (1999) (parts 1 to 3): "Information technology - Security techniques – Evaluation criteria for IT security".
6. CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".
7. IETF RFC 6283: “Extensible Markup Language Evidence Record Syntax (XMLERS)”

3 Definitions and Abbreviations

3.1 Definitions

Concept	Definition
Relying party	recipient of a time-stamp token who relies on that time-stamp token
Subscriber	entity requiring data to be time-stamped by a TSA and which has explicitly or implicitly agreed to its terms and conditions
Time-stamping authority	authority which issues time-stamp tokens
Time-stamp token	data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Long-term archive	aids in the preservation of data over long periods of time through a regimen of technical and procedural mechanisms designed to support claims regarding a data object. The long-time archive contains an Archive Hash Tree
Archive	archive of DigiStamp timestamps and the protected hash values which are then cryptographically linked to other evidence. The Archive adds greater security to our timestamps by mitigating the risk of key compromise by providing alternative means of verifying the integrity of time-stamp tokens, or other evidence that data existed before particular times.
Depository	a collection of information relevant to proving validity of time-stamp tokens and successful execution of this policy, including the Archive
Evidence Record	an Evidence Record is a collection of evidence compiled for a given archive object over time. The Evidence Record protocol used by DigiStamp is defined in RFC 6283, or referred to as XMLERS.
Archive Hash Tree	DigiStamp's Archive constitutes a Merkle forest containing individual trees which have been chained together. The resulting structure protects a multitude of datum and produces a long chain of trust that stretches back since the creation of the archive. The structure is used to create a root hash (or summary hash value) using a hash chain-link procedure.
Widely Witnessed	a technique of publishing a root hash value in various external mediums in order to fix the hash value in time and enhance the immutable quality. The result is the witnessing of the root hash value by external, disinterested parties.
Time-stamp policy	named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements
TSA Disclosure Statement	set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
TSA Practice Statement	statement of the practices that a TSA employs in issuing time-stamp tokens
End-User License Agreement	agreement between the Subscriber and DigiStamp related to the use of the DigiStamp software, Internet-based timestamp service, account access resale restrictions and other rights and limitations.
TSA Web Site	describes the current pricing of each service, tools to create timestamps and access to technical support at: www.DigiStamp.com
Repository	a place on our TSA web site where legal documents, policy statements, root certificates, the end-user license agreement, and other information relevant to our operations can be found
TSA system	composition of IT products and components organized to support the provision of time-stamping services
Time-stamping unit	set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time

Coordinated Universal time (UTC)	time scale based on the second as defined in ITU-R Recommendation TF.460-5 [1]. NOTE: For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship).
UTC	Time-scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns. (See ITU-R Recommendation TF.536-1 [2]). NOTE: A list of UTC(k) laboratories is given in section 1 of Circular T disseminated by BIPM and available from the BIPM website (http://www.bipm.org/).

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

3.2 Abbreviations

Abbreviation	Definition
TSA	Time-stamping Authority
TST	Time-stamp token
EULA	End User License Agreement
Archive	Long-term Time-stamp and Hash Value Archive
Depository	A Long-term Collection of Records Relevant to Validation, including the Archive
Repository	A Collection of Information Related to TSA Policies and Operations
UTC	Coordinated Universal Time
IETF	Internet Engineering Task Force
ESTI	European Telecommunications Standards Institute
CA	Certificate Authority
NIST	National Institute of Standards and Technology
HSM	Hardware security module

4 General Concepts

4.1 Time-stamping Services

The provision of time-stamping services is broken down in the present document into the following component services for the purposes of classifying requirements:

- **Time-stamping provision:** This service component generates time-stamp tokens.
- **Time-stamping management:** The service component that monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by DigiStamp. This service component has responsibility for the installation and de-installation of the time-stamping provision service. For example, time-stamping management ensures that the clock used for time-stamping is correctly synchronized with UTC.

This subdivision of services is only for the purposes of clarifying the requirements specified in the current document and places no restrictions on any subdivision of an implementation of DigiStamp's services.

4.2 Time-stamping Authority

DigiStamp is the authority trusted by the users of the provided time-stamping services (i.e. subscribers as well as relying parties) to issue time-stamp tokens, and is called a Time-Stamping Authority (TSA). DigiStamp has overall responsibility for the provision of the time-stamping services identified in clause 4.1. DigiStamp's key is used to sign a time-stamp token and is identified in a time-stamp token as the issuer.

DigiStamp may make use of other parties to provide parts of the Time-Stamping Services. However, DigiStamp always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. However, the private key or keys used to generate the time-stamp tokens are identified as belonging to DigiStamp.

DigiStamp may operate several identifiable time-stamping units. Each unit has a different key.

DigiStamp is a certification-service-provider, as defined in the EU Directive on Electronic Signatures (see article 2(11)), which issues time-stamp tokens.

4.3 Subscriber

The subscriber may be an organization comprising several end-users or an individual end-user.

When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.4 Time-stamp Policy and TSA Practice Statement

This clause explains the relative roles of Time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

4.4.1 Purpose

This document is publicly available. Distribution and replication of this document are limited, according to the Confidentiality Statement at the beginning and end of this document.

This document serves three primary purposes:

1) Policy: This document represents to the public WHAT guidelines DigiStamp adheres to.
2) Practice: This document represents to the public HOW DigiStamp adheres to the stated guidelines.
3) Disclosure: This document provides a set of statements to the public about the policies and practices of the TSA service that particularly require emphasis or disclosure.

4.4.2 Level of Specificity

This document is not intended to represent the entirety of the policies, standards, procedures, practices, etc., that DigiStamp adheres to. Instead, this document represents small portions of the overall population and content of the guiding documents that DigiStamp abides by, in order to convey to the public the appropriate and adequate manner in which DigiStamp acts as a TSA.

Further access to DigiStamp policies may be provided upon further request.

5 Time-stamp Policy

5.1 Overview

This policy represents a set of rules adhered to during issuance and managing of time-stamp tokens by DigiStamp.

DigiStamp issues TST with an accuracy of 1 second or less than one second, and in accordance with ETSI recommendations. Every TST includes an identifier of the applicable DigiStamp policy, described in Section 5.2 of this document, and further described in Section 7.3.1 of this document.

5.2 Identification

The object-identifier of the baseline time-stamp policy is defined in Table 1.

Table 1: DigiStamp Policy Identifier

Policy Identifier	Policy Name
iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) DigiStamp (8291) id-digistamp-time-stamping(1) OID: 1.3.6.1.4.1.8291.1.1	DigiStamp Time-Stamping Authority Policy & Practice Statement

DigiStamp includes the identifier, as an indication of our claim of conformance, to be the value of the time-stamp policy attribute within the issued TST. This Policy and Disclosure Statement is available at the repository on our website: https://www.digistamp.com/repository/about-us/repository or on request by writing to info@digistamp.com

5.3 User Community and Applicability

A timestamp is used to prove the existence of certain data before a certain point-in-time (e.g. contracts, research data, medical records, digital signatures,..) without the possibility that any party can backdate the timestamps. DigiStamp's Time-stamps are generally applicable to support a potential challenge in a court of law as the timestamp can be reliably shown to originate with systems that provide accurate results. This policy is also aimed at meeting the specific requirements of time-stamping qualified electronic signatures (see European Directive on Electronic Signatures) for long-term validity.

This policy, and DigiStamp's Time-stamp services, may be used for public time-stamping services or time-stamping services used within a closed community.

5.4 Conformance

TST issued by DigiStamp include policy identifiers as described in Section 5.2 of this document.

DigiStamp ensures compliance of provided services with regulations specified in Section 6.1 of this document and ensures reliability of control mechanisms described in Section 7 of this document.

6 Obligations and Liability

6.1 TSA Obligations

6.1.1 General

DigiStamp ensures that all TSA requirements, as detailed in Section 7 of this document, are implemented as applicable to the selected time-stamp policy.

DigiStamp ensures full conformance with the procedures described in this policy, even when sub-contractors undertake partial or entire TSA functionality. DigiStamp also ensures adherence to any additional obligations indicated in the time-stamp implicitly or explicitly.

DigiStamp provides all time-stamping services in full conformance with this document (as a practice statement).

6.1.2 TSA Obligations to Subscribers

DigiStamp takes very seriously our responsibility to meet the claims set forth in our Terms and Conditions, including the availability and accuracy of time-stamping services. DigiStamp guarantees permanent access to DigiStamp TSA services, given the course 24/7/365 excluding scheduled system maintenance, disclosed in appropriate documents, and Internet access dependencies outside of DigiStamp's control.

The time stamps produced are in accordance with common standards: in particular, RFC 3161,x.509, and ETSI TS 101 861. The operations of the time stamp service comply with the policy and practices described in the current document.

6.2 Subscriber Obligations

The subscriber needs to have adequate knowledge of digital signatures, certificates and computer technology to select and appropriately use the software needed to verify a digital signature. This present document and End User License Agreement are required as agreements to the use of the time stamp service. The EULA restricts the use of the DigiStamp software, Internet-based timestamp service, account access resale restrictions and other rights and limitations.

The Subscriber is responsible to determine if local courts will recognize the veracity and admissibility of a digital timestamp given the Subscriber's matter, local laws and customs. DigiStamp's timestamps are generally applicable to support a potential challenge in a court of law as the timestamp can be reliably shown to originate with systems that provide accurate results.

DigiStamp obligates Subscribers to verify the digital signature of the TSA upon receipt of the token. In nearly all cases, this process is facilitated automatically within the software provided by DigiStamp. The method of verifying the token is as defined in RFC 3161 Section 2.2. This includes that upon receiving a TST, the subscriber will verify the various data fields and the validity of the digital signature.

In particular:

- Verify that what was time-stamped corresponds to what was requested to be time-stamped.
- Verify that the TST contains the correct certificate identifier of the TSA.
- Verify that the policy field under which the token was issued is acceptable for the application.
- Take into account any other precautions prescribed in agreements or elsewhere.

6.3 Relying Party Obligations

The relying party assumes all the obligations of a Subscriber in Section 6.2. In addition, the relying party is directed to:

- Verify that the public key certificate has not been revoked with a reason of "key compromise." If this happens, then the time stamp is not verified, and the DigiStamp Depository may provide a means to discriminate between genuine and false tokens. If the public key has been revoked for any other reason, the time stamp is invalid if it has a time/date after the time of revocation.
- Take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy.
- Verify if cryptographic hash function used in a token is still secure, and plan to renew if necessary.
- Ensure that the size of cryptographic key of TSA and incorporated algorithm are still regarded as safe.

NOTE: DigiStamp maintains the certification revocation status for 15 years after the time stamp key is destroyed and the key signed its last time stamp. (See 7.2.4 Rekeying TSA's Key).

6.4 Liability

For more information on the burden of liability, please visit www.digistamp.com/about-us/digistamp-license-agreement/.

7 TSA Practices

DigiStamp has implemented controls that meet or exceed the following statements (in Section 7 of this document).

DigiStamp retains the right of refusal in granting a TST in response to a request that exceeds contractual service level agreements with a subscriber.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice Statement

DigiStamp takes very seriously its commitment to providing reliable time-stamping services. Management has created and implemented policies, standards, and procedures throughout the organization that govern the actions and decisions of all employees and parties associated with delivering time-stamps for DigiStamp. Specifically in this regard, DigiStamp has executed the following steps:

1) DigiStamp performs periodic risk assessments, and/or Business Impact Analyses to reevaluate the adequacy of security controls and operational procedures in place that are designed to eliminate or reduce threats to the assets with which DigiStamp operates. These risk assessments include the revisiting of all Policies and Standards in place to ensure they are up-to-date and meet appropriate industry regulations.

2) DigiStamp makes available appropriate Policy and Practice statements to the public and any review or audit organization to demonstrate compliance with ETSI TS 102 023 and IETF RFC 3628.

3) DigiStamp publishes a TSA Disclosure Statement at www.digistamp.com/about-us/repository. This TSA Disclosure Statement, in conjunction with specific, relevant contractual agreements that may exist between parties, is intended to disclose to appropriate parties the terms and conditions pertinent to time-stamping services provided by DigiStamp. This TSA Disclosure Statement is also published in Section 7.1.2 of this document.

4) The Board of Directors that serves DigiStamp acts as the management party that has final authority to approve the TSA Practice Statement that DigiStamp makes available to appropriate parties.

5) A senior management team at DigiStamp, under the direction of the CISO, is responsible for implementing and ensuring abidance by all applicable Policies, Standards, and Practices. This team is also responsible for annual review (and/or more often if needed) and modification of said Policies, Standards, and Practices, and obtains final consent from the Board of Directors prior to new releases to any party. When changes are made within the DigiStamp TSA Practice Statement due to the normal course of review, due notice of said changes will be given to all parties affected. These changes would be immediately available in the publishing of the updated Practice Statement.

7.1.2 TSA Disclosure Statement

7.1.2.1 Entire Agreement

This TSA Disclosure Statement is not the entire agreement, only a part of it. Please refer to our complete DigiStamp TSA Policy and our End-User License Agreement, available at www.digistamp.com/about-us/repository.

7.1.2.2 TSA Contact Information

The DigiStamp CISO is responsible for the development, implementation, and publishing of the DigiStamp TSA Policy and Practice Statement, and all relevant documents pertaining to time-stamping services provided by DigiStamp. All inquiries and comments concerning the contents of stated documents can be directed to:

DigiStamp, Inc.
Address: 2525 Turtle Creek Blvd #403
Dallas, TX 75219
E-mail: info@digistamp.com
Phone: 214.377.0378

7.1.2.3 Time-stamp Token Types and Usage

DigiStamp offers a single class of time-stamp token under the policy identifier 1.3.6.1.4.1.8291.1.1. Time-stamps tokens produced under 1.3.6.1.4.1.8291.1.1 are in the form prescribed by RFC 3161 and subsequent standards. These time-stamp tokens can be used for any purpose except the protection (e.g. time-stamping) of a timestamp produced by a TSA other than DigiStamp. We accept the following hash algorithms:

- SHA-1
- SHA-256
- SHA-384
- SHA-512 (recommended)
- RIPEMD-160

Our time-stamp token signatures are encrypted using RSA 2048. Each time-stamp token include the public keys necessary for verification, and can be verified against DigiStamp's root certificate or the known and published audit public key for the source time-stamping unit. Certificates can be retrieved from our Repository at: https://www.digistamp.com/repository/about-us/repository.
Looking to NIST for life expectancy estimates for our time-stamp token signatures, at the time of this writing they can be expected to remain valid through 2030. DigiStamp preserves the time stamps in an Archive for fifteen (15) years. The Archive will provide DigiStamp the ability to extend validity of all constituent time-stamps through the application of newer signatures with greater strength.

7.1.2.4 Reliance Limits

The level of accuracy of time that is provided by DigiStamp in a time-stamping token is +/- one (1) second with respect to UTC. See Section 7.3.2 of the complete TSA Policy for more information at www.digistamp.com/docs/DigiStampTSApolicy.pdf.
TSA Event Logs are maintained in our Depository for fifteen (15) years. See Section 7.4.11 of the complete TSA Policy for more information at www.digistamp.com/docs/DigiStampTSApolicy.pdf.

7.1.2.5 Obligations of Subscribers

See Section 6.2 of the complete TSA Policy at www.digistamp.com/docs/DigiStampTSApolicy.pdf.
Subscribers are also subject to the End-User License Agreement at www.digistamp.com/about-us/digistamp-license-agreement/.

7.1.2.6 Obligations of Relying Parties

See Section 6.3 of the complete TSA Policy at www.digistamp.com/docs/DigiStampTSApolicy.pdf.

7.1.2.7 Limited Warranty and Disclaimer/Limitation of Liability

See Article IV of the End-User License Agreement at www.digistamp.com/about-us/digistamp-license-agreement/.

7.1.2.8 Applicable Agreements and Practice Statement

Relevant content can be found in our Repository at www.digistamp.com/about-us/repository.
In particular, applicable agreements include Obligations of Subscribers and Obligations of Relying Parties described in our TSA Policy and Practice Statement Available at www.digistamp.com/docs/DigiStampTSApolicy.pdf. The

DigiStamp End-User License Agreement is applicable, and available at www.digistamp.com/about-us/digistamp-license-agreement/.

7.1.2.9 Privacy Policy

See Privacy Policy at www.digistamp.com/about-us/privacy-and-legal-policies.

7.1.2.10 Refund Policy

See Article IV of the End-User License Agreement at www.digistamp.com/about-us/digistamp-license-agreement/.

7.1.2.11 Applicable Law, Complaints, and Dispute Resolution Mechanisms

See Article III of the End-User License Agreement at www.digistamp.com/about-us/digistamp-license-agreement/.

7.2 Key Management Life Cycle

7.2.1 TSA Key Generation

There are two key-pairs for the operations of the TSA. One key-pair is for creating timestamps and the other is for issuing timestamp public-key certificates. Both key-pairs are generated within a hardware-based cryptographic module that complies with the FIPS 140 Level 3 or superior requirements [2]. The procedure for generating both key-pairs, securing the access methods and initializing software within the cryptographic module complies with requirements of trusted operation systems[3]. The key generation algorithm and length (RSA 2048 bit) are in accordance with standards for the purposes of time-stamp tokens.

7.2.2 TSA Private Key Distribution

The TSA private key must be created within a certified cryptographic module (see Section 7.2.1). The cryptographic module is audited to reliably prevent disclosures of the private key to any persons. The FIPS-certified tamper detection mechanisms ensure the private key is destroyed if tampering is detected. There are no backups or second copies of the TSA private keys and thus no distribution.

7.2.3 TSA Public Key Distribution

The time stamp public key is used to verify the authenticity of the time stamps that you have created using the time-stamping service. The public keys are published as x.509 certificates. The public key certificates are in the repository at: http://www.digistamp.com/about-us/repository or on request by writing to info@digistamp.com.

The same cryptographic module that creates time stamps also performs as the Certificate Authority. By using a key-pair that is stored within the cryptographic module for this purpose (see Section 7.2.1), it issues the time stamp public key certificate. The security of this certificate issuance operation is equivalent to this time-stamping policy.

7.2.4 Rekeying TSA's Key

The time stamp key-pairs are replaced frequently within the hardware device. The frequency is one year or after one million time stamps are created. Each event of "rekeying of the TSA key" results in the cryptographic module signing a new x.509 public key certificate with a validity period of two years. The previous time stamp private key is destroyed at the time of rekeying, and the public key certificates are retained for 15 years in the Depository. The certificate issuance key that is within the cryptographic module cannot be changed or rekeyed and remains until the module is decommissioned (see Section 7.2.6).

---

[2] National Institute of Standards and Technology (NIST) – Cryptographic Module Validation Program.
[3] The most common set of criteria for trusted operating system design is Common Criteria.

7.2.5 End of TSA Key Life Cycle

TSA private keys contained within the audited cryptographic module are destroyed in a manner such that the private keys cannot be retrieved. The private key has no backups nor was it ever exported or distributed (see Section 7.2.2). The TSA will reject attempts to issue a time stamp token if the signing private key has expired.

The associated public key certificates are revoked with specified reason that it has been superseded. This life cycle event is recorded as part of DigiStamp's certification revocation list[4].

7.2.6 Life Cycle Management of Cryptographic Module Used to Sign Time-stamps

The initialization of the hardware security module (HSM)[5] is a procedure to ensure that private keys are retained within the HSM for the controlled purpose of creating trusted time stamps and issuing time stamp public key certificates. The initialization procedure creates validation data that is used at a later time to prove that the HSM is still in a valid, unaltered state for creating trusted time stamps. This audited process includes external auditors to record, date, and notarize the action of initializing the HSM. This evidence is retained for the purpose of audits, reviews, and dispute resolution.

The procedure to decommission a time stamp device is done by using the manufacturers prescribed methods to erase the installed time stamp software, the Issuer Key, and time stamp key. This incorporated procedures associated with Section 7.2.5 End of TSA Key Life Cycle. The certificate issuance public key certificate is revoked with specified reason that it has ceased operations. This life cycle event is recorded as part of DigiStamp's certification revocation list.

7.3 Time-Stamping

7.3.1 Time-stamp Token

The DigiStamp TSA service produces a time-stamp token (TST) upon receiving a valid request from a subscribing party. DigiStamp returns the timestamp to the subscriber and preserves a copy the timestamp, and the hash value in the request, in DigiStamp's Archive. The form and content of the time-stamp token is compliant with the protocol defined in IETF RFC 3161 and profiled in TS 101 861. In brief, the time-stamp token combines the hash value of the user's data with the current time and then binds those together with a digital signature.

DigiStamp ensures that time-stamp tokens are issued securely and include the correct time. The time stamp key-pair is used exclusively for the purpose of creating time stamps. Each time stamp includes a unique serial number. The serial number is an integer that is incremented by one with each subsequent time stamp created using the time stamp key-pair.

The time contained with the time stamp token is synchronized with UTC and is accurate to one second. If DigiStamp TSA has not been able to maintain synchronization with UTC for any reason, then a time stamp token will not be issued.

Contained within each time stamp are the identifier for DigiStamp's time-stamp policy (see Section 5.2) and a unique identifier for the x.509 certificate that was used to authenticate the time stamp. The policy identifier is a value that is registered with IANA[6] to identify the DigiStamp organization. The identified x.509 certification contains the locality and country of DigiStamp along with an identifier for the specific HSM used to create the time-stamp token.

---

[4] As of the time of this writing, DigiStamp maintains certification revocations by publishing this information on the public web site using a manual process and does not provide an OCSP service.
[5] A Hardware Security Module is a specific type of cryptographic module
[6] Internet Assigned Numbers Authority IANA.ORG

A valid request from a subscribing party includes a token of this policy or does not include any policy token. In the case that a request includes no policy token then DigiStamp defaults to a request with token specify to use the Archive storage (OID: 1.3.6.1.4.1.8291.1.2) unless otherwise specified by agreement between DigiStamp and the subscriber.

7.3.2 Clock Synchronization with UTC

The time stamp clock is contained within the same cryptographic module as the time stamp private key (see 7.2.6). The security protection of the cryptographic module detects clock tampering and maintains a signed audit trail of synchronization events. The system detects variations from UTC reference source to maintain a clock accuracy of within one second.

7.4 TSA Management and Operation

7.4.1 Security Management

DigiStamp has implemented administrative and management procedures to, at a minimum, meet recognized industry best practices for the maintenance and preservation of security.

In particular:
DigiStamp retains responsibility for all aspects of time stamp provisioning, whether or not any functions are outsourced to subcontractors. Policies and Standards are in place to govern any such relationship, clearly defining any and all responsibilities of all third parties involved, including the security of applicable information. These Policies require that all controls defined and implemented for DigiStamp operations are also executed appropriately by third parties. As such, DigiStamp retains responsibility for the communication and enforcement of all relevant practices to all involved in delivering services for DigiStamp.

The Chief Information Security Officer (CISO) at DigiStamp is responsible for developing and implementing appropriate security policies. The CISO collaborates with DigiStamp senior management to ensure the direction of security measures implemented is in line with DigiStamp's primary business goals. The CISO is also responsible for publishing all relevant Policy, Standards, and Procedures that govern DigiStamp activities.

The CISO is responsible for the monitoring of all relevant security matters within DigiStamp locations, to ensure that operations are not interrupted for matters of security. Changes to the security infrastructure or Policy are approved by senior management quorum.

DigiStamp maintains an extensive set of Policies, Standards, and Procedures that have been implemented within the business activities of operation of the business. The security controls and operating procedures affecting facilities, systems, and information assets are published appropriately, updated annually, and available / mandated for all appropriate parties to practice. Further, these Policies direct that both business targets, and potential threats, are considered, documented, and planned for in order to minimize the negative impact of expected and unexpected events, while maximizing the opportunity to provide time-stamping services in the most reliable and secure manner possible. Risk assessments, disaster recovery plans, and other appropriate planning / assessment documents are updated annually or more often to ensure preparation for such events is adequate, tested, and reliable.

7.4.2 Asset Classification and Management

DigiStamp has committed an essential level of resources to ensuring that information and assets are appropriately protected.

In particular:

DigiStamp maintains an inventory of all assets (real and perceived). These assets are classified according to their nature, and appropriate controls are defined and implemented to ensure appropriate protection and security is practiced. Periodic risk analyses are performed to ensure full understanding of present risk and appropriate oversight.

7.4.3 Personnel Security

DigiStamp has dedicated an extensive amount of resources to ensuring that only talented and committed individuals become part of the growing DigiStamp team. Hiring practices are an important component of this commitment. DigiStamp takes very seriously its responsibility to ensure the delivery of time-stamping operations worthy of trust.

In particular:

DigiStamp employs only qualified individuals for their respective positions. Many current employees and subcontractors have a great deal of experience and expertise in their specific areas, having worked in various degrees at a combined 25% of the Fortune 500 companies. In addition, some employees are followed as leaders in the time-stamping industry. Relevant expertise and experience are considered in depth during the hiring process.

Job roles and responsibilities within DigiStamp include (if any) security and trust aspects relevant to the specific role(s), and are clearly documented and communicated within job descriptions at hiring and employment. Job roles requiring elevated levels of trust are clearly identified, and special attention is given to ensuring segregation of duties and 'least privilege' as possible to provide an environment worthy of the trust of DigiStamp customers. Job descriptions are written to be as specific as possible to the defined role, differentiating between general functions and TSA specific functions, and include skill and experience requirements.

All DigiStamp employees are required to execute the job descriptions and responsibilities assigned to them in a manner that is consistent and supportive of DigiStamp's information security management procedures (see clause 7.4.1).

DigiStamp staff, with managerial duties, are required to maintain current and relevant:

- knowledge of time-stamping technology;
- knowledge of digital signature technology;
- knowledge of mechanisms for calibration or synchronization the TSA clock with UTC;
- familiarity with security procedures for personnel with security responsibilities;
- experience with information security and risk assessment.

DigiStamp staff, in trusted roles, are required to be free, both in fact and perception, from conflicts of interest with the industry, the business, and the technologies in use. Appointment to trusted roles can be authorized only by DigiStamp senior management with responsibility for security (e.g. CISO). Trusted roles shall not be granted to persons of questionable conviction, those with previous criminal conviction, or to anyone without completion of appropriate and necessary background checks.

7.4.4 Physical and Environmental Security

DigiStamp infrastructure used to deliver time-stamping services has been designed and implemented in a fashion that reduces the chance of compromise even when physical access to the device(s) is gained. However, DigiStamp believes in and practices 'security in layers', and has taken great strides to provide redundant levels of hardware from multiple geographic regions, all from environments that include appropriate controls to minimize the chance of unauthorized access or physical damage.

In particular:
For both the time-stamping provisioning hardware, and time-stamping management:

- physical access to facilities concerned with time-stamping services is limited to properly authorized individuals;
- controls have been implemented to avoid loss, damage, and compromise of assets and interruption to business activities;
- controls have been implemented to avoid compromise or theft of information and information processing facilities.

DigiStamp utilizes a cryptographic module (IBM 4758 Coprocessor) that contains built-in physical access controls. In addition, a number of procedures at initialization of the module are designed to appropriately apply 'soft' access controls to the device (see clause 7.2.1 and 7.2.2).

The following additional controls have been applied to time-stamping management at DigiStamp:

- All 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 part(s) of the premises shared with other organizations is 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 TSA's physical and environmental security policy for systems concerned with time-stamping management address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, 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

Within DigiStamp's drive to provide reliable time-stamping services to its customers, direction and instruction to ensure all system components are secure and correctly operated and with minimal risk of failure have been drafted at the Policy, Standard, and Procedural/Practice level and communicated to all who are involved with providing the services.

In particular:

The integrity of DigiStamp system components and information is protected against viruses and malicious / unauthorized software. Specific Policy has been drafted in this regard, and implemented for all DigiStamp systems.

Incident response procedures have been documented and communicated to employees, to ensure the minimization of any potential security incident.

Appropriate access to media within DigiStamp systems has been documented and communicated, to ensure that media is protected and current. In addition, DigiStamp's information classification guidance mandates appropriate handling procedures with regard to the level of sensitivity required.

Capacity demands are monitored continuously to ensure that DigiStamp can meet the claims of availability given to all customers. Future capacity projections are updated regularly to ensure that no break in service will occur at any future point.

Incident response procedures in place at DigiStamp are designed to provide adequate guidance to ensure that all involved in a possible incident can respond quickly and appropriately to minimize potential effects on the organization and/or services. These procedures also define the reporting requirements, after the incident, to make available appropriate information to DigiStamp customers.

DigiStamp security operations are managed by trusted personnel and separated from other operations. These responsibilities include, but are not limited to:

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;

- media handling and security;
- data and software exchange.

7.4.6 System Access Management

DigiStamp has taken many steps to ensure that system access is limited to properly authorized individuals. This is consistent with and part of the 'security in layers' method that DigiStamp has implemented.

In particular:

A number of network and system based controls (e.g. certified firewalls, routers) have been implemented to protect internal network domains from unauthorized access. These controls are in continuous refinement to ensure optimization and that they remain up-to-date. Consistent with clause 7.4.4, least access requires that network protocol availability is limited only to those needed for provisioning of time stamps.

DigiStamp has implemented controls at all levels of the organization around Identity Management, for any and all users of any kind and definition. These controls are designed to ensure effective and appropriate administration of all users and all roles and responsibilities. These Identity Management controls ensure that all potential users of critical applications of any nature are properly identified and authenticated prior to use.

DigiStamp has restricted access to information and application system functions in accordance with documented access control policy statements and procedures to ensure appropriate segregation of practices between trusted and non-trusted users (e.g. system utility programs).

DigiStamp personnel will be held accountable for their activities, and monitored at a number of levels ('security in layers'). The retention, monitoring, and security of event logs (see clause 7.4.10) is one particular method of ensuring that user activity is appropriate.

Like all DigiStamp critical systems, local network components (e.g. routers, firewalls) are kept physically secure. Configurations and device logs are monitored to ensure only appropriate use occurs and changes are made. Non-time-stamping systems will also be monitored and secured within alarmed facilities to enable timely reaction to inappropriate use.

7.4.7 Trustworthy Systems Deployment and Maintenance

DigiStamp utilizes trustworthy and often certified systems and products to minimize the chance/effect of unauthorized modification.

In particular:

DigiStamp has implemented policy (i.e. "Secure Systems Design Policy", "Security in Systems Development Policy") to ensure that security requirements are considered in the initial phases of system design and specification as both integral and appropriate for optimal system development. In addition, change control standards (i.e. "Development Change Control Standard") have been implemented that govern releases, modifications, and emergency fixes of any operational software.

7.4.8 Compromise of TSA Services

DigiStamp is in the business of trust. As such, it is of the utmost importance that if the time stamps provided were compromised in any way, the customer would be notified immediately. DigiStamp would communicate this information in a variety of ways.

In particular:

DigiStamp sees the potential compromise of the private signing key and the loss of calibration of the time-stamping clock as primary risk points. The Disaster Recovery Plan, as well as the design of the systems in general, was

implemented in a manner to both prevent this risk from being realized and to provide guidance on how to proceed in the event that either happens.

In the event of a private key or clock compromise or any disaster that may potentially affect the customer, DigiStamp will communicate to the customer what has happened, what is being done to address it, and how they may be affected.

In the event of a real or suspected private key or clock compromise, DigiStamp will discontinue the issuance of time stamps until recovery procedures are complete.

If a compromise of DigiStamp's operations is confirmed, DigiStamp shall make every effort to assist potentially affected subscribers or relying parties in determining which time stamps were affected. Every effort available to DigiStamp may be utilized, so long as the privacy of each customer is maintained.

NOTE: In case the private key does become compromised, a Depository of tokens generated and maintained by DigiStamp may provide a means to discriminate between genuine and false backdated tokens.

In the case of a real or suspected private key compromise, DigiStamp will perform the following actions, as detailed in the DRP and summarized here:

- The public key certificate corresponding to the compromised key is revoked with reason of "key compromise."
- A new private key will be generated.
- Relying Parties who may be affected will be immediately informed about the compromise of the key using contact methods they have recorded a DigiStamp, by means of mass media, and E-mail.
- The associated Evidence Records from the Archive will be supplied to Rely Parties as described in section 7.4.12 Archive, without charging a fee for the operation.

7.4.9 TSA Termination

In the unexpected event that DigiStamp ceases time-stamping services, a sequence of events has been established and documented that will enable subscribers and relying parties to continue, without interruption, to verify the status of the time-stamp tokens previously issued.

In particular:

At a minimum, the following actions shall be executed before termination of service:

- DigiStamp shall make available to all subscribers and relying parties information concerning its termination;
- DigiStamp shall terminate authorization of all subcontractors to act on behalf of DigiStamp in carrying out any functions relating to the process of issuing time-stamp tokens;
- DigiStamp shall transfer obligations to a reliable party for maintaining the Depository (see Section 7.4.11) necessary to demonstrate the correct operation of DigiStamp for a reasonable period;
- DigiStamp shall maintain or transfer to a reliable party its obligations to make available its public key or its certificates to relying parties for a reasonable period;
- DigiStamp private keys shall be destroyed in a manner such that the private keys cannot be retrieved.

The DigiStamp Depository and its Archive may be made "Public" to achieve the obligation of "reliable party for maintaining the Depository". If this Public option is used then the Depository will have had removed any data to identify the specific Subscriber associated with a timestamp.

DigiStamp shall maintain funding, at all times, to at a minimum cover the costs of these actions in the event of bankruptcy or other unforeseen circumstances.

DigiStamp would take necessary steps to have applicable certificates revoked.

7.4.10 Compliance with Legal Requirements and Privacy

DigiStamp will ensure compliance with applicable legal requirements at all times.

In particular:

DigiStamp takes multiple technical and organizational measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction, theft, or damage to personal data.

DigiStamp will protect customers' privacy (see "DigiStamp Privacy Policy"). The information contributed by users to DigiStamp will be protected from disclosure unless by contractual agreement or other legal requirement (e.g. court order). The Subscriber's time stamps may be stored in the Depository (see Section 7.4.11 Recording of Information) related to the Archive. At DigiStamp's discretion the time stamps in the Depository may be published and generally available to the public. Information that associates the Subscriber with a specific timestamp is confidential and cannot be released without Subscribers permission and that information may have been permanently lost.

7.4.11 Recording of Information Concerning Operation of Time-stamping Services

The operation of the Time-Stamping Service creates and captures information that describes various operational events. DigiStamp believes that the recording of operational events is part of a "defense in depth" approach to providing trustworthy services to subscribers. In addition, this information may be of particular importance during the course of potential legal proceedings. This information is stored in the long term Depository as described below.
The procedure for a Relying Party to obtain and verify Depository information is by writing to info@digistamp.com.
DigiStamp may charge a fee for any Depository access services.

In particular, the Depository contains:

1. Archive
The Archive of Subscribers' individual time-stamps and protected hash values is preserved for the purpose that it might be used as an additional method to verify a TST in case the associated time-stamping private key was compromised, a dependent cryptographic algorithm is no longer reliable, or the datum's hash value must be verified directly against Widely Witnessed events or through some other method provided by the Archive. This Archive is described in more detail below.

2. Cryptographic Module Life Cycle Events
An initialization ceremony of the time stamping machines utilized independent third-party witnesses. The signed audit statements of these third-party witnesses are part of the Depository (see Section 7.1.2 TSA Disclosure Statement).

3. TSA key management
Records concerning all events relating to the life-cycle of DigiStamp keys are logged.
Records concerning all events relating to the life-cycle of DigiStamp certificates (if appropriate) are logged.

4. Clock synchronization
Records concerning all events relating to synchronization of the DigiStamp internal reference clocks to UTC are logged.
Records concerning all events relating to detection of loss of synchronization are logged.
Records concerning all events related to clock adjustments made to specific time stamp cryptographic module.

DigiStamp has documented the specific operational events and data to be recorded, the length of archive of these records, and the process of destruction of these records (collectively referred to as the data life cycle). The security of operational records is regarded as equivalent to other sensitive data. As such, appropriate measures are documented and taken to ensure the maintenance of confidentiality and integrity of the time-stamping operational event records.

DigiStamp will take appropriate measures to ensure that Depository information cannot be easily or mistakenly deleted or destroyed within the period of time specified for preserving the Depository. The precise event time of any significant DigiStamp operational events will be recorded appropriately for these purposes.

The length of time for preservation of operational records is fifteen (15) years. The Archive that contains the time stamps that were created for the Subscriber is preserved for fifteen (15) years. The certification revocation status is preserved for fifteen (15) years after the time stamp key is destroyed and the key signed its last time stamp. (See 7.2.4 Rekeying TSA's Key). The TSA may preserve all or portions of this data for longer periods.

If DigiStamp ceases operation of the TSA service, the 15 year preservation period may be fulfilled by publishing the Depository contents. In such an event, all information which could easily be used to correlate a timestamp or hash value with a particular subscriber will be removed from the Archive before publication.

If a key compromise occurs, or some other event impacts the ability of relying parties to verify or trust time stamps created by DigiStamp TSAs, DigiStamp will publish information from the Depository necessary for the verification and trust of affected time stamps. In such an event, all information which could easily be used to correlate a timestamp or hash value with a particular subscriber will be removed from the Archive before publication.

There is a portion of the Depository available to the general public on-line at www.DigiStamp.com. All data contained in the Depository may at DigiStamp's discretion be published as generally available to the public, such as in the public Repository at www.digistamp.com/about-us/repository.

7.4.12 Archive

The Archive is operated to provide the generic functionality of a long-term archive service for the TSA. The Archive produces Evidence Records as described in IETF RFC 6283 (XMLERS).

Service policy

When a Subscriber requests the issuance of a new time-stamp token, the TSA submits for storage these items to the Archive: 1. the hash value of the user's data and its associated hash algorithm identifier 2. The resulting time-stamp token that was created. The TSA may optionally submit additional data including information to associate the Subscriber with the request.

DigiStamp is under no obligation to successfully capture, store, and preserve time stamps or protected hash values in the Archive. However, DigiStamp does make a "best effort" to achieve 100% Archive inclusivity.

In additional to the primary source of entries to the Archive describe above, the TSA may also submit for storage timestamps that were created in other systems.

DigiStamp does not allow the deletion of archived data objects.

DigiStamp may optionally provide services to Subscribers or Relying Parties to search for and retrieve time-tokens and associated Evidence Records.

Archived data object maintenance policy

The Cryptographic Maintenance Policy for the DigiStamp Archive dictates acceptable algorithms, rules for preservation activity triggers, default archival period, and default handling upon expiration of archival period.

At the time of this writing, this policy includes the following requirements:

- Use of SHA-512 for the construction of Archive Hash Trees
- Use of RSA-2048 for protection of Archive Hash Trees
- All signing algorithms are upgraded 5 years before NIST recommendations deprecate them

- A preservation activity trigger of every 23 hours is used for routine protection
- A default archival period of 15 years
- A default handling of object expiration of: no action

Archived data object renewal

Renewal of signatures is performed every 23 hours with the largest signing keys in-use by DigiStamp time-stamping units.

The root of the most recent Archive Hash Tree is published every 31 days to achieve Widely Witnessed protection.

Renewal of the hash originally sent to DigiStamp is the responsibility of the Subscriber and/or Relying Party, not DigiStamp. Renewal of the Archive Hash Trees will be performed when preservation activity is triggered, and the hashing algorithm for Archive Hash Tree construction is upgraded.

Authorization policy

Any Party may request Evidence Records for a timestamp created by DigiStamp. DigiStamp may not provide this service for timestamps created for a Subscriber that has not abided by their obligations in this present document or the End User License Agreement.

7.5 Organization

DigiStamp takes measures to ensure that organizational practices will positively impact the provision of reliable time-stamping services.

In particular:

DigiStamp's policies, standards, and procedures/practices are non-discriminatory.

DigiStamp provides its services to any customer that agrees to abide by the stated obligations of a subscriber, as specified in the Disclosure Statement.

DigiStamp is incorporated according to the definition of national law.

DigiStamp takes great measures to ensure that its systems, quality, and management practices are not only appropriate for the provisioning of time-stamps, but that they exceed industry practices, in many cases.

DigiStamp maintains adequate arrangements, operationally and financially, to cover liabilities arising from the general course of conducting business, and to be able to conform to the statements of this policy.

DigiStamp employs a sufficient number of personnel having the necessary education, training, technical knowledge, and experience relating to the type, range, and volume of work necessary to provide time-stamping services.

DigiStamp publishes a dispute resolution procedure (see Disclosure Statement) for use by all involved in the use of DigiStamp products and services.

DigiStamp has developed policy to ensure contractual relationships with sub-contractors, outsourcers, and other third parties are appropriately defined and regulated.

Annex A (informative): Coordinated Universal Time[1]

Coordinated Universal Time (UTC) is the international time standard that became effective on January 1, 1972. UTC has superseded Greenwich Mean Time (GMT), but in practice they are never more than 1 second different. Hence many people continue to refer to GMT when in fact they operate to UTC.

Zero (0) hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal meridian. Universal time is based on a 24 hour clock, therefore, afternoon hours such as 4 pm UTC are expressed as 16:00 UTC (sixteen hours, zero minutes).

International Atomic Time (TAI) is calculated by the Bureau International des Poids et Mesures (BIPM) from the readings of more than 200 atomic clocks located in metrology institutes and observatories in more than 30 countries around the world. Information on TAI is made available every month in the BIPM Circular T (ftp://62.161.69.5/pub/tai/publication). It is that TAI does not lose or gain with respect to an imaginary perfect clock by more than about one tenth of a microsecond (0.0000001 second) per year.

Coordinated Universal Time (UTC): Time scale, based on the second, as defined and recommended by the International Telecommunications Radio Committee (ITU-R), and maintained by the Bureau International des Poids et Mesures (BIPM). The maintenance by BIPM includes cooperation among various national laboratories around the world. The full definition of UTC is contained in ITU-R Recommendation TF.460-4.

Atomic Time, with the unit of duration the Systeme International (SI) second defined as the duration of 9 192 631 770 cycles of radiation, corresponds to the transition between two hyperfine levels of the ground state of caesium 133. TAI is the International Atomic Time scale, a statistical timescale based on a large number of atomic clocks.

Universal Time (UT) is counted from 0 hours at midnight, with unit of duration the mean solar day, defined to be as uniform as possible despite variations in the rotation of the Earth.

- UT0 is the rotational time of a particular place of observation. It is observed as the diurnal motion of stars or extraterrestrial radio sources.

- UT1 is computed by correcting UT0 for the effect of polar motion on the longitude of the observing site. It varies from uniformity because of the irregularities in the Earth's rotation.

UT1, is based on the somewhat irregular rotation of the Earth. Rotational irregularities usually result in a net decrease in the Earth's average rotational velocity, and ensuing lags of UT1 with respect to UTC.

Coordinated Universal Time (UTC) is the basis for international time-keeping and follows TAI exactly except for an integral number of seconds, 32 in year 2001. These leap seconds are inserted on the advice of the International Earth Rotation Service (IERS) (http://hpiers.obspm.fr/) to ensure that, having taken into account irregularities, the Sun is overhead within 0,9 seconds of 12:00:00 UTC on the meridian of Greenwich. UTC is thus the modern successor of Greenwich Mean Time, GMT, which was used when the unit of time was the mean solar day.

Adjustments to the atomic, i.e., UTC, time scale consist of an occasional addition or deletion of one full second, which is called a leap second. Twice yearly, during the last minute of the day of June 30 and December 31, Universal Time, adjustments may be made to ensure that the accumulated difference between UTC and UT1 will not exceed 0,9 s before the next scheduled adjustment. Historically, adjustments, when necessary, have usually consisted of adding an extra second to the UTC time scale in order to allow the rotation of the Earth to "catch up." Therefore, the last minute of the UTC time scale, on the day when an adjustment is made, will have 61 seconds.

Coordinated Universal Time (UTC) differs thus from TAI by an integral number of seconds. UTC is kept within 0,9 s of UT1 by the introduction of one-second steps to UTC, the "leap second." To date these steps have always been positive.

Annex B (informative): Long Term Verification of time-stamp token

A time-stamp token can be verified beyond the end of the validity period of the certificate from the TSA. Verification of a time-stamp token can still be performed beyond the end of the validity period of the certificate from the TSA, if, at the time of verification, it can be known that:

- the TSA private key has not been compromised at any time up to the time that a relying part verifies a time-stamp token;
- the hash algorithms used in the time-stamp token exhibits no collisions at the time of verification;
- the signature algorithm and signature key size under which the time-stamp token has been signed is still beyond the reach of cryptographic attacks at the time of verification.

If these conditions cannot be met, then the validity may be maintained by applying an additional time-stamp to protect the integrity of the previous one. Alternatively or additionally the time-stamped data may be placed in secure storage.

DigiStamp maintains a Long Term Archive of Timestamps so that it may be used in the future to improve the longevity of older timestamps.

DigiStamp preserves certification revocation information for 15 years. The compromise of time stamp keys that were used by this time stamp service would have significant impact and it would be disclosed to public media and press.

DigiStamp's policy and practices are designed to create reliable and manageable digital evidence by using agreed upon methods of associating time data to transaction so that they might be compared to each other at some later time. These methods include the application of the currently accepted practices and cryptographic algorithms.

Revision History

Date	Version	Description of Change / Update	Approver
July 30, 2001	1.0	Initial Policy statement	CISO
October 18, 2008	2.1	Rewrite to comply with IETF RFC 3628	CISO
December 2012		The meaning of Policy Identifier 1.3.6.1.4.1.8291.1.1 was changed from "not saved in archive" to "saved in archive". Provisions were made for created timestamps to be checked if they are in the archive and to submit them to the archive.	CISO
December 2012		Removed description to Policy Identifier (OID) 1.3.6.1.4.1.8291.1.2. This OID was never applied to a timestamp by our system. It had been intended to indicate a timestamp that was included in the Archive.	CISO
December 2014	3.1	Significant changes including addition of archive functions and reworking of disclosure statement.	CISO