DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

TIMESTAMP POLICY
AND
TSA PRACTICE STATEMENT

VERSION 2.0 – 27/01/2021

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	*Edition n.º*	*Content*
10/04/2013	1.0	Initial drafting
21/12/2017	1.1	Revision
27/01/2021	2.0	Review and publication subsequent to the creation of new CAs

RELATED DOCUMENTS

Document Details	*Author(s)*
Certification Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	*Approved by*
Signed By: ALVARO OLIVEIRA DE MATOS Entitlement - DIRETOR GERAL Certificate Profile - Qualified Certificate - Member "DIGITALSIGN - CERTIFICADORA DIGITAL, SA" Qualified Digital Certificate - Member Electronically Signed Document. This electronic signature replaces the hand written signature in the UE.	Assinado Por: FERNANDO AVELINO LEITE DOS SANTOS MOREIRA Entitlement - ASSINAR DOCUMENTOS E CONTRATOS Certificate Profile - Qualified Certificate - Representative DIGITALSIGN - CERTIFICADORA DIGITAL S.A. Certificado Digital Qualificado - Representação Documento assinado eletronicamente. Esta assinatura eletrónica substitui a assinatura autógrafa na UE.

LEGAL NOTICE

CONTENT

1. INTRODUCTION

The purpose of this document is to define the policy, practices and procedures used in the support to the activities of Time-Stamping by the Certification Authority of DigitalSign-Digital Certification, SA ("EC DIGITALSIGN").

This document is in compliance to the Internet Engineering Task Force (IETF) RFC 3628 for Policy Requirements for Time-Stamping Authorities and may undergo regular updates.

1.1. OVERVIEW

EC DIGITALSIGN Time-Stamping service uses public key infrastructure and reliable time sources to provide reliable timestamps and in accordance with patterns globally accepted.

This document (Timestamp Policy and TSA Practices Statement) defines the practices and policies used for the operation and management of the Time-Stamping service of EC DIGITALSIGN, so that subscribers and relying parties can assess the confidence level of the operation of this service.

The aim of the Time-Stamp service is to provide timestamps used as support for qualified electronic signatures, according to Regulation 910/2014 of the European Parliament and of the Council of 23 July, and other relevant national legislation.

Nevertheless, the timestamps can also be used for any other purpose that requires proof that certain data existed at a specific time.

Practices for creation, signature and certificate issuance, as well as revocation of invalid certificates carried out by a Certification Authority ("CA") are essential to ensure the reliability and confidence of a Public Key Infrastructure ("PKI").

This document respects and implements the following standards:

- ETSI TS 102.023: *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*
- RFC 3628: *Requirements for Time-Stamping Authorities*

This Timestamp Policy and TSA Practices Statement and further fixes and / or updates are approved by the Management Group (see 9.17.1. of CPS)

Corrections and / or updates shall be published in the form of new versions of this document, replacing any previous version.

1.2. DOCUMENT DESIGNATION AND IDENTIFICATION

This document is the Timestamp Policy and TSA Practice Statement of EC DIGITALSIGN and should be read in conjunction with the current version of Certification Practice Statement (CPS) of EC DIGITALSIGN, available for viewing at: http://pki.digitalsign.pt. It was not associated any identifying object to this document.

This document is identified by the following information:

Document Information	
Version/Edition	2.0
Approval Date	27/01/2021
Expiration Date	Not applicable
Location	http://pki.digitalsign.pt

2. REFERENCES

- ETSI TS 101.456: *Policy Requirements for Certification Authorities Issuing Qualified Certificates*
- ETSI TS 101.861: *Time-stamping Profile*
- ETSI TS 102.023: *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities*
- ETSI TS 102.176.1: *Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms*
- CPS: *Certificate Practices Statement of EC DIGITALSIGN*
- RFC 3161: *Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)*

3. ACRONYMS AND DEFINITIONS

EC/CA	Certification Authority
EC DIGITALSIGN	Certification Authority of DigitalSign – Certificadora Digital, SA
DPC/CPS	Certification Practices Statement
PKI	Public Key Infrastructure
OID	Unique number of the object identifier
LCR/CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
UTC	Coordinated Universal Time
EVC/TSA	Time Stamp Authority

4. GENERAL CONCEPTS

4.1. TIMESTAMPING SERVICES

Timestamping services include the following components:

- Technical components that issue timestamps;
- Management, control and monitoring components of timestamping service, including synchronization with reliable UTC time sources.

4.2. TIMESTAMP AUTHORITY

Timestamp Authority (TSA) is trusted by its users (ie, subscribers and relying parties) to issue secure timestamps. The EC DIGITALSIGN TSA is responsible for the operation of one or more timestamp services identified in section 4.1 above.

4.3. SUBSCRIBER

Subscribers are the end users of timestamps issued by EC DIGITALSIGN TSA.

Subscribers can be individuals or organizations (public or private), as well as technological equipment.

4.4. TIMESTAMP POLICY AND TSA PRACTICE STATEMENT

This document should be read in conjunction with the current version of the Certification Practices Statement (CPS) of the EC DIGITALSIGN, available for viewing at: http://pki.digitalsign.pt, which regulates the operation of EC DIGITALSIGN and its digital certificate services.

4.4.1. PURPOSE

This document specifies the policy and practices statement for the timestamp service provided by EC DIGITALSIGN, in order to meet the safety and reliability requirements described in section 2 of this document.

For further details, see section 7.1 of this document.

4.4.2. LEVEL OF SPECIFICITY

This document describes the general rules for timestamps issuance and management. A detailed description of the system is compiled into additional restricted documents, available only to authorized personnel and auditors.

4.4.3. APPROACH

This policy has been crafted to the general level, without describing any technical details about the IT system and communications, organizational structure and operating and

protection procedures. This policy does not define the computing environment in which the service is running.

The technical details and operation can be found in the Certification Practice Statement (CPS) of EC DIGITALSIGN, described above.

5. TIMESTAMP POLICIES

5.1. OVERVIEW

This Timestamp Policy defines a set of processes for creating timestamps, according to ETSI TS 102 023.

TSA signs timestamps electronically using private keys that are specifically reserved for this purpose. The timestamps signature private keys are stored in cryptographic device (HSM) dedicated and approved.

Each timestamp contains a policy identifier and is issued with an accuracy of 1 second or more.

The timestamps are ordered via the Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP), as specified in RFC 3161.

5.2. IDENTIFICATION

The object identifier of the Timestamp Policy is: 1.3.6.1.4.1.25596.2.1.1.

This identifier is referenced in all timestamps issued by the TSA of EC DIGITALSIGN, and this policy is available to all subscribers and relying parties.

5.3. USER COMMUNITY AND APPLICABILITY

The community of users for timestamp services of EC DIGITALSIGN includes subscribers and relying parties. All subscribers are automatically considered relying parties.

EC DIGITALSIGN can provide public timestamp services.

EC DIGITALSIGN does not impose restrictions on the applicability of timestamps, with the exception of the cases referred to in the CPS.

5.4. CONFORMANCE

EC DIGITALSIGN references the policy identifier in section 5.2 (Identification) of this document in all timestamps issued to indicate compliance with this policy.

EC DIGITALSIGN is subjected to independent external and internal audits, in order to demonstrate that the timestamp service fulfills the obligations defined in section 6.1 (TSA Obligations) and has implemented appropriate controls as described in section 7 (Requirements on TSA Practices).

6. OBLIGATIONS AND LIABILITY

This chapter describes the duties, responsibilities and guarantees of the TSA, subscribers and relying parties.

6.1. TSA OBLIGATIONS

6.1.1. GENERAL

EC DIGITALSIGN operates the TSA and assumes the responsibility of the requirements described in section 7 (Requirements on TSA Practice) of this document, as well as the provisions of applicable national and European legislation.

These duties and responsibilities are regulated by mutual agreements signed between the parties, where the Timestamp Policy and TSA Practices Statement (this document) and Certification Practice Statement (CPS) are integral parts.

6.1.2. TSA OBLIGATIONS TOWARDS SUBSCRIBERS

DigitalSign assumes the following obligations towards the subscribers of the timestamp service:

- Its timestamp activity is based on certified equipment and software.
- It operates in accordance with the Timestamp Policy and TSA Practices Statement (this document) and Certification Practice Statement (CPS), as well as other relevant policies and procedures.
- It ensures that the timestamps maintain an accuracy of at least one (1) second relative to UTC.
- It undergoes audits and internal and external assessments to ensure compliance with relevant legislation and policies and procedures adopted.
- It provides an high-availability access to the systems for obtaining timestamps, except in cases of technical programmed interruptions, loss of time synchronization and other cases described in Section 9.8 (Limitations of Liability of the CA) of the CPS.

6.2. SUBSCRIBER OBLIGATIONS

Subscribers must ensure that the timestamps have been properly signed, and check the CRL to confirm that the private key used for signing these timestamps is not compromised.

Subscribers must use the standard RFC 3161 to request timestamps.

6.3. RELYING PARTY OBLIGATIONS

Before trusting a timestamp, relying parties must verify that it was properly signed, as well as check the CRL to confirm that the private key used for signing this timestamp was not compromised.

The relying party should take into account possible limitations of using timestamps indicated in this document, as well as the precautions provided in this document and other referenced.

During the validity period of the timestamp certificate, the status of its private key can be verified by consulting the CRL. If the timestamp check is performed after the validity period of the certificate, relying parties shall proceed in accordance with the requirements of Annex D of the ETSI TS 102 023.

6.4. LIABILITY

DigitalSign is committed to operate the timestamp service in accordance with this Policy and the Certification Practice Statement (CPS), as well as the agreements between the parties.

DigitalSign doesn´t assume any expressed or implied responsibility or guarantee for (except in cases of agreements) the availability or accuracy of the timestamp service.

7. REQUIREMENTS ON TSA PRACTICES

The issuance of timestamps, in response to an issuance request, is at the discretion of DigitalSign and depends on the accordance of the subscriber.

7.1. PRACTICE AND DISCLOSURE STATEMENTS

7.1.1. TSA PRACTICE STATEMENT

This Timestamp Policy and TSA Practices Statement establishes the general rules relating to the operation of the TSA.

CPS and other internal documents define how DigitalSign meets the technical, organizational and procedural requirements identified in this Timestamp Policy and TSA Practices Statement.

Public documents, including this document and the CPS, can be found in DigitalSign repository at: http://pki.digitalsign.pt. Internal documents may be provided only on strictly controlled conditions.

EC DIGITALSIGN carries out risk assessments to determine threats and set security controls and required operational procedures.

7.1.2. TSA DISCLOSURE STATEMENT

This Timestamp Policy and TSA Practices Statement, along with the CPS, are the publicly available documents, as described in section 7.1.1 of this document.

This document shall disclose to all subscribers and relying parties the terms and conditions of timestamp service of DigitalSign. A synthesis of the elements of the TSA Disclosure Statement is presented below:

- The timestamp service is operated by EC DIGITALSIGN, and is duly accredited by Autoridade Nacional de Segurança, as legally stipulated.
- Contact information are referred in section 1.5.2 of CPS.
- Each timestamp issued by EC DIGITALSIGN contains a policy identifier, as described in section 5.2 of this document.
- The cryptographic algorithms and key size are used in accordance with ETSI TS 101 861 standards, and are commonly:
    - *hash* algorithms accepted in applications: SHA1, SHA256, SHA384, SHA512.
    - Signature algorithms: sha256WithRSAEncryption (2048 bit key)
- DigitalSign does not establish other confidence limits beyond the disposed in section 6.3 above. DigitalSign will inform, by appropriate means, subscribers and relying parties in the case of cryptographic algorithms and / or the key sizes used are no longer considered safe.
- Subscribers' obligations are described in section 6.2 of this document.
- Relying parties obligations are described in section 6.3 of this document.
- DigitalSign keeps records related to the operation of the timestamp service, in accordance with the provisions of section 5.5 of the CPS.
- The DigitalSign may charge fees for the timestamp services

7.2. KEY MANAGEMENT LIFE CYCLE

This Timestamp Policy and TSA Practices Statement, along with the CPS, are the publicly available documents, as described in section 7.1.1 of this document.

7.2.1. KEY GENERATION

DigitalSign generates the cryptographic keys used for timestamps signature in HSM device, certified according to FIPS 140-2 Level 3, by authorized personnel in a secure physical environment.

The algorithms and key size used are described in section 7.1.2 of this document.

7.2.2. PRIVATE KEY PROTECTION

DigitalSign adopted specific measures to ensure that private keys used for timestamps signature remain confidential and maintain their integrity. These measures include the use of HSMs certified according to FIPS 140-2 Level 3 or higher.

When backup copies of these keys are made, this procedure is performed by authorized personnel, requiring at least a dual custody, and secure physical environment. Any backup is always performed for encrypted file or directly to another cryptographic equipment (HSM).

7.2.3. PUBLIC KEY DISTRIBUTION

Digital certificates used by the timestamp service are issued by EC DIGITALSIGN respecting the practices, policies and procedures described in CPS, providing a level of safety equivalent to this timestamp policy.

Additional information can be found in section 6.1.4 of CPS.

7.2.4. KEY RENEWAL

DigitalSign requires, for this purpose, the creation of a new pair of keys to replace the expiring key pair (technically defined as «re-key», but in this document identified as «renewal»).

Keys are renewed before the expiry of its validity period.

7.2.5. KEY DESTRUCTION

keys used by the timestamp service are replaced after its expiry. Timestamps are not issued using the expired keys. After its expiry, the private keys are destroyed.

7.2.6. LIFE CYCLE MANAGEMENT OF THE CRYPTOGRAPHIC MODULE

DigitalSign adopted specific measures to ensure that cryptographic modules (HSMs) used in non-repudiation services are not violated in the transport or storage.

All HSMs are reinitialized before use, by authorized personnel and in a secure physical environment.

Whenever an HSM is submitted to technical intervention or disabled, all the keys stored are cleared (zeroisation) according to the manufacturer's instructions.

7.3. TIME-STAMPING

7.3.1. TIMESTAMP

In accordance with the protocols referenced in Section 2 of this document, each timestamp includes, but is not limited to:

- A representation (hash value) of the data that are validated chronologically according to subscriber's information.
- A unique serial number;
- A timestamp validation policy identifier;
- The time value;
- A qualified electronic signature generated by using the private cryptographic key for the exclusive use of the TSA.

7.3.2. CLOCK SYNCHRONIZATION

The time used is defined according to the Coordinated Universal Time (UTC) and certified by a national measurement institute, with an uncertainty of less than 100 milliseconds (ms).

7.4. TSA MANAGEMENT AND OPERATION

7.4.1. SECURITY MANAGEMENT

All matters related to the security management are listed in Section 5.2 of CPS.

7.4.2. RISK ASSEMENT

To ensure that all the information assets are subjected to an appropriate risk treatment, DigitalSign maintains an inventory of assets, with the corresponding risk ratings, in order to perform a consistent risk analysis.

7.4.3. PERSONNEL SECURITY

All matters relating to personnel security management are set out in section 5.3 of CPS.

7.4.4. PHYSICAL AND ENVIRONMENTAL SECURITY

All matters relating to physical and environmental security are set out in section 5.1 of CPS.

7.4.5. OPERATIONS MANAGEMENT

EC DIGITALSIGN implements an extensive set of controls in accordance with ETSI TS 102 023, which are part of the internal documentation.

EC DIGITALSIGN is submitted to independent external and internal audits, in order to demonstrate that the timestamp service fulfills all obligations laid.

Additional information on the management of operations can be found in Section 5 of CPS.

7.4.6. SYSTEM ACCESS MANAGEMENT

All matters relating access management to the systems are referred to in sections 5 and 6 of CPS.

7.4.7. TRUSTING ENVIRONMENT

Issues related to the trusting environment are listed in Section 6 of CPS.

7.4.8. COMPROMISE OF TSA SERVICES

In case of compromised private cryptographic key used in the timestamp service, DigitalSign shall follow the procedures described in section 5.7 of the CPS. This includes the revocation of the appropriate digital certificate and its inclusion in the CRL.

In case of loss of clock synchronization, and if this means a loss of accuracy assumed, DigitalSign stops issuing timestamps signature until calibration is again within the defined parameters. In the event that the issuance of time stamps is detected with an accuracy that does not comply with that specified in section 7.3.2, DigitalSign will use commercially reasonable efforts to notify the subscribers and affected third parties affected.

7.4.9. TSA TERMINATION

In case of TSA extinction, DigitalSign shall follow the procedures described in section 5.8 of the CPS. This includes at least the information to subscribers, the revocation of the digital certificates used in the timestamp service and the transition of services for a successor CA, ensuring that the entity to which all documentation is transmitted, undertakes its maintenance during the period of time legally required.

7.4.10. LEGAL REQUIREMENTS

DigitalSign operates in accordance with the applicable European and Portuguese standards, as well as in strict compliance with the provisions of Chapter 7.4.10 of the ETSI TS 102.023

7.4.11. AUDIT RECORDS

The system used by DigitalSign in timestamp service incorporates tools for collection and processing of audit records.

7.5. ORGANIZATIONAL

The organizational structure, policies, procedures and controls of EC DIGITALSIGN are applied to timestamp service.