
# Certdigital Policy of

# Time Stamping Services

| **ISSUED BY:** | | |
|---|---|---|
| **DEPARTMENT** | **NAME** | **DATE** |
| **MANAGEMENT OF POLICIES AND PROCEDURES** | **TECHNICAL DIRECTOR** | 09.04.2012 |

| **APPROVED BY:** | | |
|---|---|---|
| **DEPARTMENT** | **NAME** | **DATE** |
| **CERTIFICATE CALIFICATE** | **TECHNICAL DIRECTOR** | 09.04.2012 |

| **HISTORY OF MODIFIERS:** | | | |
|---|---|---|---|
| **VERSION** | **AUTHOR** | **MODIFICATION DETAILS** | **DATE:** |
| 1.0.0 | **COMPARTMENT CHIEF** | The first version of the document | 09.04.2012 |
| 1.1 | **TECHNICAL DIRECTOR** | Changes according to Regulation (EU) 910/2014 | 08.05.2017 |
| | | | |

# Content

# 1. Introduction

## 1.1. Mark CertDigital

CertDigital is the trademark under which S.C. Centrul de Calcul S.A. Provides certification and time stamping services. Every time CertDigital refers to the contents of this document, those references involve the S.C. Centrul de Calcul S.A.

## 1.2. Content

The "Time stamping policy" document defines the practices and working procedures implemented by S.C. Centrul de Calcul S.A. (Henceforth referred to as "CertDigital") as a provider of time stamping services under Regulation (EU) No. 910/2014 and Law no. 451/2004 on the temporal mark for the purpose of providing time stamping services.

By the nature of the services provided, CertDigital ensures the confidentiality of the processing of the personal data of the clients through a confidentiality statement agreed by the parties.

This document includes among the practices and working procedures defined issues such as:

- Obligations and responsibilities of the time stamping authority, respectively users of time stamping services;
- Legal issues regarding the provision of time stamping services by CertDigital;
- Key life cycle management
- How to manage the Time stamping policy.

The detailed description of the practices and procedures for time stamping services is presented in the DPSMT Statement of Practice.

Knowledge of the Temporary Stamping Service Policy and the Statement of

Practice of Time Stamping Services is of particular importance to CertDigital's subscribers and partner entities.

# 2. Time stamping policy

## 2.1. Time stamping

Through the time stamping service, CertDigital provides:

- Timeline Branding Services;
- Quality control services for time stamping services to meet predefined quality standards in this document.

In the time stamping process, the user sends CertDigital a time stamping request for an electronic document. This request contains the fingerprint of the document for which the request is made, the fingerprint created by applying a hash-code function to the document. CertDigital applies the time information, referring to the time base and signs electronically using a qualified digital certificate, resulting in the time stamp that is transmitted to the user.

## 2.2. Time stamping authority

By fulfilling the regulations related to Regulation (EU) No. 910/2014 and Law no. 451/2004 on the time stamping and its applicable rules, CertDigital defines its framework for providing time stamping services to subscribers and assumes full responsibility for the provision of these service.

CertDigital generates and signs time stamps through a Time Stamp Authority (TSA).

The information system implemented by CertDigital allows the continuous provision of time stamping services and ensures that it is impossible to issue

a correct mark for another time than when the document was received or to change the order in which the time stamps are issued.

### 2.3. Obligations

#### 2.3.1. Obligations of the Authority for Timestamping

By means of a policy assumed and made available to users, CertDigital's time stamping authority attributes a number of fundamental obligations as follows:

- Establishment of a document (in particular, Time stamping policy) to define the working method, the applicable procedures, the general policy of the Company, the obligations and rights of the contracting parties, etc. to be approved by the Leadership and published in an environment accessible to users to whom it is addressed;

- Carry out the activity in accordance with the procedures described in this document;

- Implementing reliable hardware and software resources that support the smooth running of the business on a permanent basis based on the imposed regulations, as well as from the business point of view in the virtual environment;

- Generate functional pair private key - public key, and protection of private key by using a secure cryptographic device, by adopting the necessary measures to prevent the unauthorized loss, disclosure, modification, or unauthorized use of the private key that is solely used for the purpose of applying for electronic signature on timestamps issued;

- Creating and maintaining an electronic record of time stamp records, including the timing of the time stamps;

- Provide users with the software required to use the time stamping

service and information related to: the conditions under which the software, user instructions, user obligations, or any other limitations on the use of the software are available;

• Allocation of personnel with the specialized knowledge, experience and qualification required to provide time stamping services;

• Keeping the time stamps for 10 years;

• Keeping the documentation related to algorithms and procedures for generating issued time stamps;

• Provide a free online check of time stamps;

• Ensure permanent access to the time base;

• Informing users about the terms and conditions regarding the use of time stamping services. In this respect, CertDigital offers users the following information through their own website http://www.certdigital.ro:

- CertDigital contact details;

- the applied time stamping policy;

- applicable technical standards;

- precision of time in the time stamps;

- limitations in using the time stamping service;

- user obligations;

- information on how to check the temporal mark and possible limitations on the shelf life;

- information on the protection of personal data;

- the amount of time that CertDigital events are stored;

• Ensuring the protection of personal data in accordance with Law no. 677/2001 on the protection of personal data and Law no. 506/2004 on the

processing of personal data and the protection of privacy in the electronic communications sector;

- Informing users about their obligations under this document, but also about the risk they incur by not complying with these obligations;

- If the activity ceases, the time stamping service provider CertDigital undertakes to transfer to another time stamping service provider or, as the case may be, to the Authority, the Registry of Time Trademarks, as well as the documentation related to the generation algorithms and procedures of the time stamps issued.

### 2.3.2. Obligations of the user

This document is an integral part of the contract between the Service Provider of Timeliness and the user of these services. Thus, based on this agreement, the user expresses agreement on the rules specified in this document and is subject to the following obligations:

- Subject to the rules and procedures described in this document.
- Provide information about its identity.
- Using the time stamping application made available by CertDigital.
- Authentication of the time stamp obtained by verifying the CertDigital digital signature. CertDigital holds the certificate corresponding to the public key, based on which the signature on the time stamp is verified.
- Verifying the trust and validity of the certificate with which the trademark was signed.

## 2.4. Responsibilities

In accordance with the regulations regarding the liability of the providers of marking services under Regulation (EU) No. 910/2014 and Law no. 451/2004 on the time stamp, CertDigital, as a Provider of Time Stamping Services, is responsible for the damage caused to any person who bases his conduct on the legal effects of those time stamps:

- With regard to the accuracy, at the moment of the release of the time stamp, of all the information it contains;
- As regards ensuring that, at the time of issuing the trademark, the supplier identified in it contains the trademark data generated by the time stamp verification data provided by this law;
- Regarding the fulfillment of all the obligations stipulated in chapter 2.3.1.

CertDigital's time stamping service provider must have insurance financial instruments to cover the damage it may cause in the course of time-related activities.

CertDigital is not responsible for damages resulting from the use of a time stamp in violation of the restrictions contained therein.

## 2.5. Confidentiality

CertDigital's proprietary information is obtained, stored and processed in accordance with Law 677/2001 on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data, Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector and other legal regulations in force.

The use and processing of personal data by CertDigital is strictly done to the extent that this activity is necessary for the time stamping services.

CertDigital provides all protection against unauthorized access to personal data.

### 2.6. Intellectual property rights

The Policy is the intellectual property of CertDigital.

CertDigital owns all intellectual property rights on Qualified Certificates issued by it, and reproduction of certificates is permitted only with the CertDigital.

The key pairs corresponding to CertDigital Qualified Certification Authority certificates are the property of CertDigital.

The key pairs corresponding to the signatories' certificates are the property of the signatories specified in these certificates.

# 3. Key life cycle management

## 3.1. Generate the TSA key

TSA keys are generated within a security hardware module in accordance with the standard NIST FIPS 140-1 Level 3 by trustworthy staff with trustworthy functions.

The private key cannot be deducted in any way from its public key pair.

## 3.2. TSA privacy keys protection SA

### 3.2.1. Standards for cryptographic modules

CertDigital uses cryptographic modules that are certified FIPS 140-1 Level 3 and meet industry standards for random number generation.

Keys used by the CertDigital Time Stamping Authority are generated and stored in hardware security modules (HSMs) that can only be activated by two people at a time, and which is also validated by FIPS 140-1 Level 3.

### 3.2.2. Control multi-people of private key access

CertDigital services use hardware modules that require more people to engage in sensitive tasks. All the tools required to perform these operations are safely stored and cannot be accessed without the information held by authorized persons.

### 3.2.3. The entrance of private key in the cryptographic module

CertDigital private keys are generated and stored on validated FIPS 140-1 Level 3 hardware security modules, in which, moreover, they will be used.

### 3.2.4. Activate private keys

Activation of CertDigital Private Keys issued requires password authentication and/or PIN authentication.

Users are solely responsible for the protection of private keys that they own. CertDigital has no responsibility for generating, protecting or distributing these keys.

CertDigital suggests its users authenticating using powerful passwords to prevent unauthorized access to and fraudulent use of private keys

### 3.2.5. Disable private keys

Private keys stored on a hardware security module are disabled when the card is removed from the device.

In the case of a user, disabling the primary key is done when you exit the application when the session closes.

During use, hardware security modules should not be left unattended or in any other state that could favor unauthorized access. When not in use, modules must be stored in a locked location that benefits from increased security.

## 3.3. Distribution of TSA public keys

The public keys corresponding to the TSA certificates are published on the CertDigital site at: https://ca.certdigital.ro/tsag2/

## 3.4. Destroy the private key

In its original form, destroying the primary key means removing it from the storage medium in a manner that ensures that there are no key fragments

that could allow it to be reconstituted.

Hardware Security Modules (primary and back-up) are re-initialized according to the hardware manufacturer's specifications. If this procedure fails, CertDigital assumes the obligation to destroy the equipment in a way that does not allow the recovery of the private key.

### 3.5. Security Hardware Mode Management

For security hardware, the CertDigital Time Stamping Authority applies the following checks:

- Checking security seals when delivering the equipment;
- Store the equipment in a secured area with limited access to authorized persons
- Installing and initiating by trusted people;
- Deleting and destroying the keys in accordance with the manufacturer's recommendations for decommissioning.

### 3.6. Synchronization with time base

CertDigital's time stamping service provider uses the time information of the unique time-based provider, namely the MCSI Official Time System.

The time source used by CertDigital is synchronized with the time reference provided by the single time provider with a maximum deviation of +/- 1 second. On this line, CertDigital implements calibration measures for the equipment so that the value of the abovementioned deviation is not exceeded.

### 3.7. Structure of the time stamp

The time stamp used has the following structure:

A. Information about the actual time stamp

- Version
- Policy
- Fingerprint
- Unique serial number
- The exact time of the issue

B. Signature of the supplier

- Info signature

C. Status of PKI

- PKI status code

### 3.8. Certificate Profile

The profile of a public key certificate that is used by the Time Stamping Authority complies with the IETF recommendations in RFC 3161 and is of the following form:

| Field name | Value or limit value |
|---|---|
| Version | Version 3 |
| Serial number | Unique value for each issued certificate |
| Signature algorithm | Object identifier of the algorithm used for signing the certificate (hash-code SHA-256 and RSA encryption algorithm) |

| | | |
|---|---|---|
| Issuer (Distinguished Name) | The name (CN)= | |
| | Organization (O)= | |
| | Country (C)= | |
| Not before (the date of entry into force): | Date of certificate validity started on the basis of the timing of the server with the official time of Romania | |
| Not after (expiration date) | Certificate expiration date expired based on server synchronization with Romania's official time. The validity of the certificates is established in accordance with the mandatory provisions. | |
| Subject (Distinctive name) | The distinctive name meets the requirements of the X.501 standard. Certain attributes in the Distinct Name component may be optional. | |
| Information about the public key of the topic | Coded according to RFC 2459<br>Provides information on RSA public keys. Key size is 2048 bits. | |
| Signature | Generated and encoded in accordance with RFC 2459 | |

## 4. Operational Electronic Register of Time Stamps

CertDigital maintains an Operational Electronic Register of Timestamp Records including the timing of the time stamps in accordance with the requirements of Law 451/2004 on the Temporal Mark and its Implementing Rules. This registry highlights all of the time stamps issued by the CertDigital Temporary Stamping Service Provider, and includes, in addition to the actual time stamp, also data on the trademark and the certificate used. Also, within the CertDigital Records register includes recordings of events occurring in the computer system used to generate time stamps. This register is permanently available for consultation on the CertDigital web site: https://ca.certidigital.ro/tsag2/.

All this information related to the Operational Electronic Register of Time Stamping is kept for a minimum of 10 years.

## 5. Updating the policy

CertDigital's Time Stamping Policy may change periodically. These changes will be available to all subscribers through CertDigital's Web site. Users who do not accept the changes made to the Time Stamping Policy must provide an information to CertDigital about to give up the time stamping services offered by CertDigital.