CERTDIGITAL
semnează sigur

General policy of time stamping

Reference:	1/2012
Version:	1.0.0
Page:	21
Distribution level:	General Audience

1. Terms and Definitions

Access	The possibility of using an information resource based on an acquired right
Employee	Any person who has a commitment relationship with CertDigital under a signed employment contract.
Authentication	Validating the identity of a user or entity. The authentication process verifies whether the entity is the one claiming to be and, depending on the result obtained, whether or not access to the requested resources.
The Time stamping authority (TSA)	Reliable institution that provides time stamping services through a computer system
Certificate	Data collection in electronic form proving the connection between the electronic signature verification data and a person, confirming the identity of that person
Qualified certificate	Certificate issued by a certification service provider under the conditions stipulated in art. 18 of Law no. 455/2001 on electronic signature
Private key	Unique digital code generated by a hardware and / or specialized software device. In the context of digital signatures, the private key is the data for the creation of the electronic signature, as they appear in the law
Public key	Digital ID, the private key pair required to verify the electronic signature. In the context of the digital signature, the public key represents the verification data of the electronic signature, as they appear in the law
Confidentiality	It is a security principle that restricts data access only to authorized persons.
Encryption	Transforming clear text into encrypted text to hide the content of information to prevent unauthorized modification and use.

Electronic data	Representations of information in a conventional form appropriate to the creation, processing, transmission, receipt or storage of information by electronic means
Key generator	Cryptographic equipment used to generate cryptographic keys
Hash-code	Function that returns the fingerprint of an electronic document
Internet	It is a multitude of computers connected in a global network that allows data sharing (from academic institutions, research institutes, private companies, government agencies, individuals, etc.) that can be accessed remotely
Hardware security mode	Hardware equipment controlled by software that performs cryptographic operations (including encryption and decryption)
Distinct name (ND)	A group of information of an entity that makes up a distinctive name distinguishing itself from other similar entities
Web page	Electronic document available through the Internet
Pair of keys	A complementary pair of encryption keys generated by the Certification Authority and formatted in a private key and a public key. The public key is distributed in a certificate issued by the Certification Authority
Password	Unique character string associated with a user in order to validate their identity.
Period of validity	The period between the date of entry into force of the certificate and the expiry date or the date when it is revoked
Trusted person	Permanent or temporary employee of the organization owning trusted infrastructure management rights within the organization
Electronic signature	Group of data in electronic form attached or logically associated with other data in electronic form and serving as identification method
SHA-1	Secure hash-code algorithm

User	A certification service user who, based on a contract with a certification service provider, hereinafter referred to as a provider, has a key public key public key pair and has a proven identity through a digital certificate issued by that provider

2. General framework

2.1. CertDigital mark

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.A. Calculation Center.

2.2. 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 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.

2.3. Sponsor of the procedure

The current document is under the sponsorship of CertDigital.

2.4. Audience and applicability

The scope of the Time Stamping Policy includes all participants in CertDigital time stamping services, namely subscribers, distributors or other contracting parties.

This document establishes the framework of rules and principles applicable to time stamping services used in any situation in which it is necessary to accurately establish the existence of information at a certain time.

This process involves the use of public key cryptography, digital certificates and reliable time sources.

This document defines the requirements for CertDigital's time stamping authority to provide time stamping services.

2.5. 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.

2.6. Time stamping authority

By fulfilling the regulations related to 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 services.

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.

2.7. Applicable regulations

The practices and procedures described in this document in this document have been developed in accordance with the following legislative acts:

- Law no. 451/2004 on the timestamp;
- Order 492/2009 on the technical and methodological norms for the application of Law no. 451/2004 on the timestamp
- Law no. 455/2001 on electronic signature;
- Law no. 677/2001 for the protection of individuals with regard to the processing of personal data and the free circulation of such data;
- Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

2.8. Contact address

Address: Str. Tudor Vladimirescu, no. 17, Targu-Jiu, Gorj

county E-mail: sediu@centruldecalcul.ro

Phone: +40 253 214 767

Fax: +40 253 214 767

Further information on the Timing Policy can be obtained by e-mail at sediu@centruldecalcul.ro.

2.9. Runtime

The program of the CertDigital headquarters is set between 8:00 and 16:00 with the possibility of prolongation in the situations where this is necessary.

3. Policy of time stamping

3.1. Framework

This document is a set of rules applicable for the provision and management of time stamps, but also for regulating the security level of the Time Stamping Authority.

CertDigital time stamps are issued with one second accuracy.

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

Name field	**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 (SHA-1 hash-code function and RSA encryption algorithm)	
Issuer (Distinctive Name)	Name (CN)=	
	Organization (O)=	
	Country (C)=	
Not before (the date of entry into force):	Date of Certificate Validity Validation Start Date Based on Server Synchronization with the Official Time of Romania	
Not after (expiration date)	Certificate expiration date expired based on server synchronization with the official time of Romania. 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
Signature	Generated and encoded in accordance with RFC 2459

3.2. Application

This document does not define limits on the use of time stamps issued under this policy. The time stamping authority may provide public time stamping services for: electronic transactions, archived data, electronic signatures, etc.

4. General Provisions

This chapter regulates the obligations and responsibilities both from the point of view of the time stamping authority and from the perspective of users in terms of subscribers and partner entities.

The obligations and responsibilities set forth below are governed by mutual agreements established between the parties under the applicable legislation.

4.1. Obligation

4.1.1. Obligations of the Authority for Timestamps

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 a private key public key private key and private key protection 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.

4.1.2. 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.

4.2. Responsibilities

4.2.1. Responsibility of the Time Stamp Authority

In accordance with the regulations regarding the liability of the providers of marking services under 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 2.1.1.

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.

4.3. 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.

4.4. Intellectual property rights

This Code of Practice and Procedures 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.

5. Key life cycle management

5.1. Generate the TSA key

TSA keys are generated in a NIST FIPS 140-1 Level 3 security hardware module by trustworthy, trusted.

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

5.2. TSA privacy keys protection

5.2.1. 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 Tag 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.

5.2.2. Control many-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.

5.2.3. Enter a private key in the cryptographic module

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

5.2.4. Activate private keys

Enabling 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.

5.2.5. 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.

5.3. Distribution of TSA public keys

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

5.4. 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.

5.5. Security Hardware Mode Management

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

- Checking security seals when delivering the equipment;
- Installing and initiating by trusted people;
- Deleting and destroying the keys in accordance with the manufacturer's recommendations for decommissioning.

5.6. 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.

5.7. 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

6. 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 Marking 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: ca.certidigital.ro/tsa.

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

7. Administration of the document

7.1. The mechanism of change

Changes that may occur in the content of this document are either caused by non-conformities following process reviews or periodic improvements in operational flows within CertDigital.

Implementing changes updates the document version number and date of issue of the Time stamping policy based on the date the changes were made.

CertDigital grants the right to make changes to the content (correction of printing errors, modification of published URL links, changes in contact information, etc.) on the rules of the Time stamping policy.

Revisions to this document with no impact or insignificant impact on signers and trusted parties using certificates issued by CertDigital and relevant information related to the status of the certificate can be made and recorded without notifying users and trusted parties and not involving changing the version number of Document or date of entry into force.

With the synthesis of the changes to be implemented, the Time stamping policy enters into an internal approval procedure based on a committee made up of the Director-General, the Deputy General Manager and the Managers of the Technical Departments.

Responsibility for the maintenance of this document is assigned to the department manager who provides the provision of time stamping services. For approval, the Time stamping policy is submitted to the Regulatory and Supervisory Authority, within 10 days, to be published and marked as valid.

The current version of the Time stamping policy is dated May 2011.

7.2. Approval procedure for the Time stamping policy

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.