CERTDIGITAL
semnează sigur

Code of Practice and Procedures of The Time Stamping Authority

„Cert Digital Time Stamping Authority”

Reference: 1/2012

Version: 1.0.0

Page: 32

Distribution level: General Audience

ISSUED BY ::			
DEPARTMENT	NAME	SIGNATURE	DATE
CERTDIGITAL	DEPARTMENT HEAD		12/06/2012

APPROVED BY:			
DEPARTMENT	NAME	SIGNATURE	DATE
CERTDIGITAL	DEPARTMENT HEAD		12/06/2012

HISTORY OF MODIFIERS:			
VERSION	AUTHOR	DETAILS OF MODIFICATIONS	DATE:
1.0.0	DEPARTMENT HEAD	PUBLICATION OF THE FIRST VERSION	12/06/2012

Content

Terms and Definitions

Access

The possibility of using an information resource based on an acquired right

Administrator

User who is authorized to use accounts administrative or privileged to perform their service duties. Generally, the administrator has the right to manage other types of users.

Employee

Any person who has a commitment relationship with CertDigital under a signed employment contract.

Conformity audit

Periodic review performed on certain processes, which establish the degree of compliance with the required standards

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.

Certification Authority

Reliable institution issuing certificates eligible applications. For this process, the Certifying Authority checks the information specified by the applicant in the application for certificate issuance.

Registration Authority

Institution that is responsible for identifying and authenticate the subject of a certificate

Request for issuance of a certificate

Electronic document containing details of the certificates to be created by the Certification Authority and registered by the Registration Authority

Certificate

Data collection in electronic form proving the link between 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

Digital certificate

Identification form the electronics used to authenticate and certify a user's identity when remote accessing resources.

Certificate revoked

Public Key Certificate included in the Certificate Revocation List

Valid certificate

Public Key Certificate issued by an Authority Certification, accepted by the applicant and not subjected to the revocation process

Private key

A 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

Code of Practice and Procedures

Document regulating the certification service delivery activity

Contributor

Any person who has a commitment relationship with CertDigital on the basis of a collaboration agreement signed between CertDigital and CertDigital or between CertDigital and the company for which the person works

Compromise

A violation of a security policy that leads to Loss of control over sensitive information

Privacy	It is a security principle that restrains data access only to authorized persons.
Access control	Limiting and verifying access to systems Information technology to eliminate their unauthorized use
Encryption	Transforming clear text into encrypted text to hide the content of information to prevent unauthorized modification and use.
Data in electronic form	Representations of the information in a form Conventional, appropriate for the creation, processing, transmission, receipt or storage by electronic means
Device for creating electronic signature	Software systems and / or hardware configurations, used to implement electronic signature creation data
Entity	Term used to describe a customer. For example, an entity may be a company, a trust, or an individual
Extensions	Extension fields in X.509 v.3 certificates
Firewall	It is a piece of equipment or a set of equipment configured to provide filtering, encryption or trafficking between different security domains based on predefined rules
Certification service provider	Trusted authority that provides services for creating, signing and issuing certificates
Key generator	Cryptographic equipment used to generate Cryptographic keys
Hash-code	Function that returns the fingerprint of an electronic document

HTTPS

An HTTP-like client-to-server communication protocol that allows web pages to be viewed in a secure way based on the encryption of the information transmitted by the server and decryption by the client, using the server certificate accepted at the initiation of the connection.

Information Security Incident

Accidentally or intentionally triggered event that alters information and/or equipment and causes partial or complete loss of confidentiality/integrity of information or unavailability.

Integrity

A security principle that ensures that information and information systems are not changed accidentally or intentionally.

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

List of Canceled Certificates

Document issued at certain time intervals specifying certificates that have been revoked or suspended before expiry of the period of validity. The information specified in this list includes the name of the issuer, the date of publication, the date of the next update, the serial numbers of the revoked or suspended certificates and the reasons why they were revoked or suspended.

Hardware security mode

Hardware equipment controlled by software that performs cryptographic operations (including encryption and decryption)

Distinct name (ND)

Information group 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
Pair of asymmetric keys	Pair of keys in a relationship where the private key defines the private transformation and the public key defines the public transformation.
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
PKI	Public Key Infrastructure
PKCS (Public-Key Cryptography Standards)	Cryptography standard for public keys
PKCS#10	The standard syntax for certificate applications and public key encryption standard # 10, developed by RSA Security Inc.
Information Security Policy	The policy behind CertDigital's approach to issues related to Information Security Management.
Security of Information	Confidentiality, integrity and availability of information and assurance of authenticity, responsibility, non-repudiation and accuracy of information in order to ensure business continuity, minimize risks and maximize operational profit and business opportunities.

Signatory

The person specified as the subject of the certificate holding the private key of the public key in the certificate.

Electronic signature

Attached electronic data group or logically associated with other electronic data and serving as the identification method

SHA-1

Secure hash-code algorithm

Intrusion Detection System (IDS)

System used to detect unapproved access in a network or workstation.

Asymmetric signature system

A system based on asymmetric techniques in which private transformation is used for signing and public transformation is used for verification.

SSL

Private communication channel between a WEB server and client browser

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

CDTSA

Cert Digital Time Stamping Authority

TSS

Time Stamping Service

1. General framework

1.1. CertDigital stamp

CertDigital is the registered stamp of S.C. Centrul de Calcul S.A. to provide certification and time stamping services. Every time CertDigital refers to the contents of this document, those references involve the Centrul de Calcul S.A..

1.2. Content

The "CDTSA Code of Practice and Procedures" defines the practices and working procedures implemented by S.C. Calculation Center S.A. (Hereinafter referred to as "CertDigital") in the provision of time stamping services operated under the name of "Cert Digital Time Stamping Authority" (CDTSA) in accordance with the applicable legal provisions.

1.3. Sponsor of the procedure

The current document is under the sponsorship of CertDigital.

1.4. Audience and applicability

The scope of the TSA Code of Practice and Procedures includes all CertDigital Certification and Time Marking Services subscribers, subscribers, distributors, or other contracting parties.

2. Private key management

2.1. Generate the CDTSA key pair

2.1.1. Key features of CDTSA

The CDTSA key pair is generated using the RSA algorithm and its size is 1024 bits, the electronic signature being made in combination with the SHA-1 cryptographic summary.

2.1.2. The procedure for generating the CDTSA key pair

The CDTSA key pair is generated at the CertDigital location by the System Administrator and in the presence of the CertDigital department head supervising the entire procedure. Key generation is done on a hardware security device (HSM) in accordance with FIPS 140-2. The private key is permanently stored on this device and is not available outside of the device in unencrypted form.

Both the CertDigital department manager and the administrator will record and sign the operations performed during the key pair generation. Records are kept for audit purpose.

2.1.3. Protection of CDTSA private keys

The storage of the CDTSA private keys is carried out by means of FIPS 140-2 on secured equipment, certified to comply with the provisions of Law no. 455/2001 on electronic signature and cannot be falsified. To prevent any unauthorized access or tampering of sensitive information, CertDigital implements appropriate, periodically reviewed controls to ensure proper operation.

2.1.4. Backup of the CDTSA private key

Cert Digital Time Stamping Authority is part of CertDigital's trustworthy chain as a sub-authority of Cert Digital Non-Repudiation CA Class 4. CertDigital keeps a copy of the root keys and all sub-authorizations, backed up and maintained as specified in the Code of Practice and Procedures. The CDTSA key prerequisite is not maintained in backup, in case of emergency procedures, it will be regenerated, the corresponding certificate being revoked and published in the crl.

2.2. Cert Digital Time Stamping Authority public distribution

Private Key certificates used for signing time stamps by the CDTSA are available on the www.certdigital.ro website in the Trust / Chain section.

2.3. Change the CDTSA key pair

The validity period of the certificate for the CDTSA private key is 2 years. At least 30 days before the CDTSA certificate expires, a new pair of keys and a new certificate will be generated. The CDTSA key pair will be changed to any revocation of the certificate, regardless of the reason for the revocation.

3. CDTSA specifications

3.1. Applicable technical standards

The timestamp structure is in compliance with SR ETSI TS 101 861 V1.2.1: 2005 Timeline Stamp Protocol (TSP): IETF RFC 3161.

Timeliness policy was created based on SR ETSI TS 102 023 V1.2.1: 2005 Electronic signatures and infrastructures (ESI). Policy requirements for time stamping authorities.

The digital certificate profile issued for Digital Time Stamping Authority honors the IETF recommendations in RFC 3161 and RFC 2459, Internet X.509 Public Key Infrastructure Certificate.

The Security Hardware Module (HSM) used in the CDTSA complies with the NIST FIPS 140-2 Security Requirements for Cryptographic Modules.

In creating the electronic signature of time stamps, the IETF RFC 2630 Cryptographic Message Syntax.

Timestamp time format is in accordance with IETF RFC 3339, Date and Time on the Internet: Timestamps.

The SHA-1 algorithm is defined in FIPS Pub 180-2, Secure Hash Standard. The MD5 algorithm is defined in RFC 1321, The MD5 Message-Digest Algorithm. The RIPEMD-160 algorithm is defined in ISO / IEC 10118-3, Hash-functions - Part 3: Dedicated hash-functions.

The sha1WithRSAEncryption algorithm is defined in IETF RFC2437 - PKCS # 1: RSA Cryptography Specifications Version 2.0.

Security Management CDTSA is provided according to ISO 27001: 2005, Information technology - Security techniques --

Information security management systems - Requirements and ISO 27002, Information technology - Security techniques - Code of practice for information security management.

3.2. Time

The application serving the CDTSA permanently checks synchronization of the local time server with the time base represented by the computer system meant to provide the official time of Romania.

Synchronization with the time source is permanently monitored and any non-synchronization is immediately signaled to the administrators.

The software application that emits the time stamps is made in such a way that any non-synchronization that goes beyond the assumed precision of stopping stamping. However, if it is found that time stamps have been issued that violate the assumed accuracy, both the subscribers who have received those marks and the surveillance authority are notified.

3.3. Time stamping process

3.3.1. Structure of the time stamp

The structure of the time stamp complies with the legal norms in force at the date of publication of the current version of this document, namely Law 451/2004 and Order 492/2009 with amendments and additions until the date of publication of this document.

In this regard, the time stamps includes:

- Imprint of the electronic image of the document at the time of stamping
- Information about the time stamping service provider as well as the authority that issued the time stamp (ex: DN[C,O,OU,CN], SERIAL)
- The temporal value of the mark

3.3.2. Client application for time stamping

CertDigital offers its customers free CertDigital Signer Timer. This software allows you to sign a document using a qualified certificate, temporarily mark this signature and check a signed pdf or p7s file.

Verification of the tracking file:

- Integrity of the document
- The validity of the qualified certified fingerprint for the signed document
- Integrity of the time stamp
- Validity of the trademark timestamp for the signed document
- The validity of the certificate with which the time stamp has been signed

The CertDigital Signer application automatically creates the document fingerprint that will be used in the process of generating the temporal mark by means of an algorithm that guarantees the uniqueness of the fingerprint against the electronic document and its state at the moment of the fingerprint generation. The fingerprint is a mathematical representation of the image and state of the document that cannot be used to reconstruct the original document.

3.3.3. Time stamping service

Generating and delivering time stamps is done automatically through an online service. This service, referred to as TSS (Time Stamping Service), is responsible for processing time stamping requests, checking the structure of time stamping applications, generating the time stamp and delivering it to the customer.

TSS is a service that can only be used on a logged-in basis, based on username and password.

4. Operational practices and procedures in the IT field

4.1. Physical access control procedure

The rules on which access control measures are based start from the principle that all rights are generally restricted if there is no explicit approval or authorization in accordance with CertDigital policies and procedures.

4.1.1. Location of location

CertDigital Headquarters is located in Tudor Vladimirescu Street, no. 17, Targu-Jiu, Gorj County.

4.1.2. Protection against unauthorized access

The Certification Authority's office is equipped with an alarm and access control system (stand-alone DVR, surveillance cameras, access control, proximity reader, motion sensors, smoke and alarms).

CertDigital has entered into a contract with a specialized security firm to ensure the intervention of a crew within 6 minutes of receipt of the anti-burglary, fire or panic alarm.

The Certification Authorities' equipment room is additionally protected by a metallic anti-burglary door, accessed by a magnetic card, by entering a security code and by operating a key, devices that only the system administrator and the CEO can act on.

4.1.3. Physical access

The CertDigital management identifies the access rights required by employees and communicates these rights to the responsible staff for implementation in accordance with the procedures in force.

Access to the premises is based on the following rules:

- Every employee CertDigital has full access to his office;
- Throughout the duration of the program, each employee has access to all areas except the areas that the responsible manager has marked as restricted areas;

  Access rights for collaborators, consultants, cleaning staff, etc. Is only allowed in the areas where it is deployed activity. Access will be made by specifying the place and time required and will be approved by the responsible manager;
- Visitors are only allowed to access in reception areas and access to secured areas will be done only on the basis of a clearly defined need for the activity and

permanent oversight of a CertDigital employee;

- IT staff issues recommendations on access rules for consultants and collaborators of each department who have a business relationship with third parties.

4.1.4. Environmental controls in critical IT areas

The following measures were implemented to establish optimal conditions in critical IT areas:

- Air conditioning systems and rack mounted fans that provide optimal operating temperature for IT equipment;
- UPS equipment that serves all critical hardware devices in providing time stamping services: servers, HSM, router, firewall, internet switches and modems;
- Connection to a separate electrical grid to provide protection against overvoltage;
- To avoid possible threats (such as floods), the equipment is placed in a raised rack that is protected by a key lock.

Smoke detection systems and fire extinguishing systems.

4.2. Security policy

The security measures implemented by CertDigital that ensure the timely marking activity in optimal conditions are shared in:

- measures to ensure redundancy for critical data;
- measures to ensure the continuity of the services offered;
- protective measures against the mistakes of the hired personnel;

4.2.1. Measures to provide redundancy for critical data

Mirroring system for server hard drives: Data security is provided by systems based on RAID matrices Mirroring forms duplication of data providing protection against physical loss of information.

Time stamping clustering system: The server that hosts the time stamping service is set to work in clustering with another backup server, thus ensuring a high level of availability of services.

Systematic Backup Process: Time stamp data is saved and archived periodically in accordance with the provisions of the rescue and restoration procedure.

4.2.2. Measures to ensure the continuity of the services offered

In order to ensure continuity of services offered, CDTSA has an Internet connection through two lines provided by different providers, as follows:

- RDS - 2 MB main fiber optic line guaranteed;
- Romtelecom - 20MB back-up line of ADSL.

4.2.3. Romtelecom - 20MB back-up line of ADSL

Qualified staff in certification activities

The staff of the CDTSA is made up of qualified people with a wealth of professional experience and possessing certifications and diplomas.

The personnel involved in the CDTSA processes must provide proof of the fulfillment of the past requirements, qualifications and experience required to perform competently and satisfactorily the job responsibilities.

- Activities are assigned according to the responsibility sheet so that a more complex activity can be carried out only with the consent of more people. An example would be the creation of new key pairs and certifications for certification authorities, where the system administrator and the management authority responsible for the certification should collaborate as specified in the operational procedure governing this activity. Moreover, for critical activities, the written consent of the Director General is required.

4.3. Data rescue and restoration procedure

The rescue program is developed on the basis of a risk assessment carried out by CertDigital's IT staff.

The system administrator is responsible for the entire back-up and restore process, which must be performed according to the current procedures. For the restraining procedure it is necessary, however, a written authorization, signed by the CertDigital Management.

4.3.1. The rescue process

At the CDTSA level, two sets of critical data are identified.

- The SQL Server database, where all the issued time stamps are kept;
- CDTSA key pairs stored on the Hardware Security Module (HSM).

The backup process is done by the System Administrator, which includes both points in the above paragraph.

The SQL Server database back-up process is run automatically, programmatically, using native SQL Server programs (back-ups) in the following steps:

1. **Full Back-up - runs weekly each Sunday at 00.00**. Backup consists of completely saving the database: tables, structure, views, stored procedures and functions, indexes, resulting in an exact copy of the initial database at the time of saving. Saving is done on Network Storage in a file called "ca_full_backup.bak".
2. **Differential Back-up** is automatically executed daily, once at 1.00, and consists of saving all changes in the database that have occurred since the last Full Backup. Saving is done on Network Storage in a file called ca_diff_backup.bak.
3. **Transaction Log Back-up** is automatically executed daily from 8:00 to 18:00, every two hours, including time intervals. This procedure saves the log of operations on the SQL database. Saving is done on Network Storage in a file called "ca_log_backup.bak".

Saving HSM data is performed on the manufacturer's Smart Cards, the information is encrypted and distributed in a redundancy scheme. Smart cards are safely held in an external location authorized for storing values.

Every Friday on weekdays, Network Storage saves are written on CD / DVD magnetic media, stating the date and time at which they were saved. Subsequently, the CD / DVD drives are stored in a safe place in key-protected metal lockers and dedicated security system from CertDigital.

4.3.2. Restoration procedure

The implementation of restoration procedures is carried out as follows:

- The IT department performs at least quarterly testing of the back-up environment to verify that it can be used to restore data.
- Restore testing - is performed on the test environment and aims to verify the correct operation of the restored data.

If hardware failures (motherboard malfunction, storage failure, or other) are identified, the problem is remedied by replacing defective components with other compatible new components with the same technical characteristics as those of the original components.

After installing the new components in the system, if necessary, repopulate with existing data saved before the problem occurs. To back up the data backup procedure (CD or DVD), the written consent of the Director General.

The restoration process will be performed by the system administrator under the supervision of the Technical Director, who will be responsible for this process.

4.3.3. Follow-up procedure for compromising the private key of the CDTSA

In case of compromising the private key of CDTSA, or in the case of suspicion of such a compromise, the following measures:

- A new pair of keys and a new certificate will be generated.
- The old certificate will be revoked and published in the Revoked Certification List.
- Active customers will be notified by electronic mail of this event.

4.4. Account management procedure in CertDigital systems

All user accounts of CertDigital employees are uniquely identified by a username (based on the employee's name using the account) and a password (which will be determined based on the rules and procedures mentioned in the Procedure for administering the passwords).

The user name of an employee is issued during the course of his activities under contract with CertDigital and can only be modified on the basis of well-founded needs (the employee changes his name legally, CertDigital carries out another employee with Similar or similar names that can create confusion, etc.).

CertDigital's computer and e-mail applications allow the definition of user groups that specify the rights that the users in a group have in using a computer system. User groups will be defined in accordance with the strict responsibilities and requirements that the category of users to associate with.

Users have the obligation to use their access rights in computer systems that have been granted only to fulfill their assigned tasks and responsibilities, and it is forbidden to use the information to which they have access for purposes other than those specified.

It is also forbidden for employees to alienate or "lend" their own access accounts to the computer network, computer applications or e-mail systems to other employees.

A user's account may have multiple states as follows:

- *Active - your account is fully operational*;
- *Expired - the account password is expired and reactivation is required to generate a new password*;
- *Disabled - the use of the user account has been suspended due to termination of the employment contract between the employee and the Company or if the account holder no longer fulfills the criteria for using the account*.

4.4.1. Creating user accounts

Defining user accounts for CertDigital's computer network, computer systems, or e-mail systems is done by application management personnel within the IT Department.

When hiring a new person in CertDigital who needs access to one or more of the IT systems, the direct boss will ask for the creation of the required user accounts by filling out a form for creating a user account. The form will detail the applications and systems for which the access account is requested, as well as the rights and user profiles that that person needs in order to fulfill the responsibilities assigned to him / her.

The completed form must be signed both by the user and by the direct superior and must be submitted to the IT Department for implementation.

Based on the completed form and its approval, the IT Department will create the required accounts exactly with the rights and profiles specified.

4.4.2. Changing User Accounts

If there is a need to modify an access account in CertDigital IT systems, the requesting user will complete a user account modification form by specifying in detail the new rights they require (applications and computer systems, profile User, etc.) as well as the rights it holds and which must be canceled with the change of position within CertDigital.

The completed form is approved by the direct superior of the employee who will agree and review where appropriate the details of the requested user accounts, as well as of those that will be canceled.

Based on the completed form and its approval, the IT Department will perform the operations to modify the accounts in accordance with the specified details.

Also, if the activity is interrupted for more than 60 days (for example in the case of maternity leave), the employee has the obligation to request through the user account modification form the temporary deactivation of the user account. The form must be signed by the supervisor directly and sent to the IT Department that will act accordingly.

4.4.3. Disable user accounts

The process of disabling a user account is based on the liquidation letter issued by the Human Resources Department. Thus, upon termination of the employment contract with CertDigital, the employee will submit to the IT Department the liquidation file containing a reference to the deactivation of his user accounts.

The IT department will deactivate accounts immediately or as soon as possible to mitigate the risk of keeping an active account inappropriately and will confirm this by signing the winding up.

In order to facilitate the traceability of activities performed with user accounts, they will be disabled and not deleted. After a period of at least 24 months after deactivation, the IT Department may decide to permanently delete the accounts.

4.5. The administration procedure for users with privileged rights

A privileged right is the unrestricted access of a user's implemented controls to one or more functionalities within a computer system.

These rights include, but are not limited to:

- A user with administrator rights;
- The right to directly access the application databases;
- Access rights on specific system facilities (applications, utilities).

The allocation of privileged rights for users in the Company's IT applications is allowed only on the basis of an authorization and a justified need in the job description in the case of employees, respectively in the service / collaboration contracts for third parties.

Beneficiaries of privileged rights are, in general, system administrators, network administrators, system engineers, or third-party consultants who require access to CertDigital's IT applications to undertake specific actions (such as maintenance, maintenance, debugging, etc.).

Privileged rights are identified for each element of the infrastructure (for example, operating system, database, etc.) and for each application. Also, the categories of users for whom these rights will be assigned are also identified.

Certain emergency situations may justify the use of privileged accounts. Thus, a preconfigured access privilege is made and appropriate control imposed. For example, user account access data can be stored in a sealed envelope in a secure location, along with a list of people authorized to use these accounts if necessary. Also included in the sealed envelope are the contact details of the system administrator to be contacted when opening the envelope.

4.5.1. Managing user accounts with privileged rights

Application management personnel are responsible for creating, modifying, and deleting user accounts with privileged rights. The process of creating an account with privileged rights based on an issued request implies, in addition to the usual process and described in the procedure of account management in CertDigital systems.

The privileged user accounts must be permanently reviewed by the Security Officer in order to prevent the situation in which unused active accounts or inappropriate access rights may exist in the system.

System administrators, if possible, should not use accounts with privileged rights to conduct day-to-day low-level activities. For these activities, each administrator must hold an account with normal access rights in parallel.

4.5.2. Monitor user accounts with privileged rights

All activities deployed through user accounts with privileged rights will be monitored and recorded. According to the retention policy, these files will be saved and kept for a specified period of time and will be reviewed periodically or whenever needed by the Security Officer. It will draw up regular reports containing the results of the review process.

4.6. Password management procedure for CertDigital personnel

The purpose of this procedure is to set standards for password creation, protection and frequent change, so that the CertDigital information system is protected against unauthorized access.

Passwords are associated with user accounts and are used in CertDigital applications or applications (for example, for network access, e-mail, etc.). Therefore, it is necessary for all employees to know the recommendations regarding the choice of appropriate passwords.

4.6.1. Rules for choosing passwords

Appropriate passwords have the following features

- Contains both capital and lowercase letters (a-z, A-Z);
- Continue digits and at least one alphanumeric character (0-9,! @ # $% ^ & * () _ + | ~ - = \ `{} []:;
- There are no words spoken in any language, dialect, slang, jargon etc;
- It is not based on personal information such as names, phone numbers etc;
- Does not coincide and does not contain the username;

• They have a minimum length of eight characters.

Inappropriate passwords are passwords of low complexity that are often characterized by one of the following specifications:

• It is a commonly used word, such as:

- The words "CertDigital", "Bucharest", "password" or other derivatives;

- The name of the family user, children, service colleagues, pets, etc;
- Birthdays, addresses, phone numbers, car number or other personal information;
- Words or sequences of letters or numbers like: abcdef, 123456, zyxwvuts, 123321 etc;
- Any of the above words written in reverse order;

• They have words that are found in a dictionary (Roman, English etc);

• Coincide or contain your username;

• They are less than eight characters in length.

4.6.2. Protecting passwords by users

Passwords associated with user accounts are not used for authentication in CertDigital external systems (for example, personal email accounts, merchant sites, etc.). Also, passwords are chosen distinctly for each type of application that requires password authentication.

All passwords are classified as confidential and are not allowed to be stored in computer systems or on another medium.

If password-related controls are not being met, CertDigital takes appropriate steps to comply with them.

4.7. Information security procedure

For optimal information handling, simplification of information security decisions and minimization of information security costs, CertDigital has implemented a hierarchy of information based on confidentiality. The main purpose of this hierarchy is to provide a consistent process of manipulation of information, regardless of how the information is presented, to whom it is addressed or who is in custody.

Each employee must have access only to the information required to perform his / her duties. Sensitive information must only be accessed by employees whose ownership of the application has been granted access.

CertDigital information should not be used for purposes other than those officially approved by the Management. Unauthorized use of restricted information is forbidden. The policy applies to all types of information within CertDigital. The policy applies to all parties that come into contact with CertDigital information, including external collaborators.

Users are not allowed to perform any activity on internal computer systems that could damage the CertDigital image.

CertDigital uses three categories of information classification detailed below.

4.7.1. Public Information

This information is approved by the CertDigital Management as public. Unauthorized disclosure of public information is permitted because it cannot cause problems to CertDigital, its customers or business partners. (Example of information publishes brochures and materials on the official website). For information to be classified as public, it must be labeled as such under the permission of the Information Owner.

4.7.2. Internally used information

Use of this information is allowed within CertDigital, and in some situations also within affiliated organizations (CertDigital partners). Unauthorized disclosure of this type of

Information to people outside CertDigital is not allowed and can cause problems within the organization, customers or business partners. This type of information can be disseminated within CertDigital without the prior approval of the Information Owner. (Examples of internal information: CertDigital phone numbers and e-mail address addresses).

4.7.3. Restricted information

It represents the most sensitive information and requires permanent monitoring. It is subject to the highest level of confidentiality. Unauthorized disclosure of this type of information to employees not needed may constitute a violation of applicable laws and regulations and may cause problems for your organization, customers, or business partners. The owner of the information may approve access to this type of information. (Examples of restricted information: merger and acquisition plans and legal information protected by lawyer-client privacy).

4.8. Personnel procedure

4.8.1. Past experience, qualifications, experience and acceptance

Staff who are nominated to be part of the Qualifying and Issuing / Qualifying Team must provide proof of the fulfillment of past experience, qualifications and experience required to perform competently and satisfactorily the job responsibilities.

4.8.2. Procedures for checking the previous references

CertDigital makes the following checks on the previous references of the staff who will handle the issue / revocation of Qualified Certificates and Time stamps:

Confirmation of the previous job;

- Verification of professional references;
- Confirmation of the highest or relevant institute of education followed;
- Studying the criminal record
- Searching for financial reports;
- Searching for driving license reports;
- Searching for social assistance reports;

To the extent that any of the imposed requirements cannot be met, CertDigital will use an investigative technique that is permitted by law and provides similar information.

Factors involved in checking the past, which can lead to the rejection of candidates to be part of the team or to take action against those in the team, include:

- Wrong presentation by the candidate;
- Personal or unfavorable personal references;
- Sentencing;
- Indices of lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, which determine the appropriate course of action, depending on the type, importance and frequency of behavior revealed by the past.. These actions may include measures that may result in the conclusion of contractual reports with that person. Using the information found by checking the past to do so is subject to the laws in force.

4.8.3. Preparation requirements

CertDigital provides staff with the necessary training to perform competently and satisfactorily the job responsibilities. CertDigital's training programs are tailored to individual responsibilities and include the following:

Basic concepts about public key infrastructure;

- Responsibilities of the function;
- CertDigital security and operational policies and procedures;
- Use and operation of existing hardware and software;
- Reporting and dealing with incident and compromise cases;
- Disaster Recovery and Business Continuity Recovery Procedures.

4.8.4. Requirements and frequency of training courses

CertDigital provides training and upgrading for staff, to the extent possible and with the frequency to ensure that the level required for the fulfillment is maintained competence and satisfactory service responsibilities. Periodic security training is provided.

4.8.5. Sanctions for unauthorized actions

Appropriate disciplinary measures are taken for unauthorized actions or other violations of CertDigital policies and procedures. Disciplinary actions may include measures that lead to the conclusion of the contract and are taken in accordance with the frequency and severity of the actions.

4.8.6. Requirements for staff contracting

Under limited circumstances, independent contractors or consultants may be employed to perform trustworthy functions. Any such contractor or consultant is maintained according to the same functional and security criteria that apply to CertDigital, which is in a similar position. Independent contractors and consultants who have not completed the past verification procedures specified in paragraph 1.2 may access CertDigital secure locations only if escorted and supervised directly by trusted persons.

4.8.7. Documentation provided to staff

CertDigital staff involved in the operation of CertDigital public key infrastructure services should read the code of practice and procedures and internal security policy. CertDigital offers its employees the necessary training and other documentation to fulfill competently and satisfactorily the responsibilities of the function.

5. Administration of the document

5.1. 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.

The implementation of the changes updates the document version number and date of issuing the TSA Code of Practice and Procedures according to 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 TSA Code of Practice and Procedures.

Revisions of the TSA Code of Practice and Practice without impact or insignificant impact on signatory and trusted parties using CertDigital certificates and the appropriate status information related to the status of the certificate can be made and recorded without notifying users and trusted parties and not involving change The version number of the document or the date of entry into force.

Along with the synthesis of the changes to be implemented, the TSA Code of Practice and Procedures shall be subject to the internal approval procedure, based on a committee composed of the Director-General, the Deputy General Manager and the Managers of the Technical Departments.

The responsibility for maintaining the TSA Code of Practice and Procedures is assigned to the department manager who provides certification services. For approval, the TSA Code of Practice and Procedures is forwarded to the Regulatory and Supervisory Authority following within 10 days to be published and marked as valid.

The current version of the TSA Code of Practice and Procedures is dated June 2012.

5.2. The mechanism of publication and notification

The TSA Code of Practice and Procedures Code is available electronically on the CertDigital website at www.certdigital.ro or may be requested by e-mail at sediu@centruldecalcul.ro.

Through the online public information display interface, CertDigital offers two versions of the document:

- Current version;
- Previous version;

Security documents considered confidential by CertDigital are inaccessible to the public.

5.3. Procedure for approving the TSA Code of Practice and Procedures

The Code of Practice and Procedures is considered valid as of its publication on the CertDigital site.

Users who do not agree to the updated version of the TSA Code of Practice and Procedures and related changes are required to make a statement to that effect within 15 days of the validation of the new version. In this case, CertDigital assigns the right to terminate the contract for the provision of the certification services and the revocation of the certificate issued on its basis. Subsequent to 15 days after the release of the new version, CertDigital considers user acceptance implicit.