Practice codes and procedures

Reference: 1/2011

Version: 1.0.1

Pages: 67

Distribution level : General Audience

ISSUED BY :			
DEPARTMENT	**NAME**	**SIGNATURE**	**DATE**
CERTDIGITAL	DEPARTMENT HEAD		17/3/2011

APPROVED BY:			
DEPARTMENT	**NAME**	**SIGNATURE**	**DATE**
CERTDIGITAL	DEPARTMENT HEAD		17/3/2011

HISTORY OF MODIFIERS :

VERSION	**AUTHOR**	**MODIFICATION DETAILS**	**DATE:**
1.0.0	DEPARTMENT HEAD	PUBLICATION OF THE FIRST VERSION	17/3/2011
1.0.1	DEPARTMENT HEAD	PUBLICATION OF THE SECOND VERSION	30/05/2015

Content

Terms and Definitions

Access	The possibility of using an information resource based on an acquired right
Administrator	A user who is authorized to use administrative or privileged accounts to perform their service tasks. 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.
Compliance audit	Periodic review of certain processes, which establishes 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 for 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 authenticating 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 provided for in Art. 18 of Law no. 455/2001 on electronic signature

Digital certificate	It is an electronic identity document 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	Certificate of public publication by a Certification Authority, accepted by the applicant and not subject 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
Collaborator	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 the loss of control of sensitive information
Confidentiality	It is a security principle that restricts data access only to authorized persons.
Access control	Limiting and checking access to information systems to eliminate unauthorized use of information systems
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
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	A 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	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 that is accepted when the connection is initialized.
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	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
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 Information Security Management issues.
Security of Information	Keeping confidentiality, integrity and availability of information and ensuring authenticity, accountability, non-repudiation and accuracy of information 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	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
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

1. General framework

1.1. CertDigital brand

CertDigital is the registered trademark of S.C. Centrul de Calcul S.A which provides certification services. For this file's content, each reference to CertDigital implies a reference to S.C. Centrul de Calcul S.A

1.2. Content

The "Code of Practice and Procedures" document defines the practices and working procedures implemented by S.C. Centrul de Calcul S.A. (Henceforth referred to as "CertDigital") in the process of providing certification services, namely issuing and administering digital certificates in accordance with the applicable legal provisions.

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 aspects such as: The obligations and responsibilities of both the certification and registration authority and the digital certificates users;

- Legal aspects regarding the provision of certification services by CertDigital;
- The mechanisms implemented to confirm the identity of the entities that applied to obtain a certificate;
- Description of operational procedures for issuance and administration of certificates;
- CertDigital Security Policy Audit and Review Processes;
- Physical access, security, personnel, and key management controls implemented by CertDigital;
- List of issued certificates, as well as the list of certificates revoked by CertDigital;

- How to administer the Code of Practice and Procedures.

1.3. Sponsor of the procedure

The current document is under the sponsorship of CertDigital.

1.4. Audience and applicability

The scope of the Code of Practice and Procedures includes all participants in CertDigital Certification Services, namely subscribers, distributors or other contracting parties. This document describes processes related to Qualified Security Certificates for CertDigital users that allow third parties to participate in the electronic communication process to verify digital signatures. Validation of a digital signature or transaction by interacting with the CertDigital digital certificate does not depend on where the certificate is issued or where the digital signature is used or the geographical distribution of the user or certification authority.

1.4.1. Certification Authority

Certification Authorities are all entities that issue qualified certificates under their own code of practices and procedures, which, depending on the ACP purpose (primary certification authority), may be the same for each ACP, or may differ from one ACP to another. Certification authorities issuing certificate end-users or other certification authorities are subordinated to the ACP.

Registration Authority

The registration authority is any CertDigital partner specifically mandated by him to carry out verification and confirmation or rejection processes for digital certificate registration, issuance, renewal or revocation applications.

If the applicant submits the request for registration, issue, renewal or revocation of digital certificates directly to CertDigital's headquarters or through the computer systems provided by him, the Registration Authority will in this case be CertDigital.

By verification, the application data is reviewed for the purpose of authenticating the applicant. In the event of cancellation of a subscriber's application for registration or withdrawal of the certificate, the Registration Authority may submit requests to the corresponding Certification Authority - to cancel the application for registration of a user and to withdraw his / her certificate.

1.4.2. End users

The scope of end-users includes both digital subscribers and partner entities that use subscriber certificates to authenticate their electronic signatures.

CertDigital digital certificates are provided for any type of user based on applicable legal limits.

1.5. 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. 455/2001 on electronic signature;
- Government Decision no. 1259/2001 regarding the approval of the technical and methodological norms for the application of Law no. 455/2001 regarding the electronic signature, with the subsequent amendments;
- Directive 1999/93 / EC of the European Parliament and the European Council and concluded on 13 December 1999 establishing the Community framework for electronic signature, as subsequently amended and supplemented;
- Law no. 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.

1.6. 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 about the Code of Practice and Procedures can be obtained by e-mail at sediu@centruldecalcul.ro.

1.7. Runtime

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

2. General provisions

This chapter regulates the obligations and responsibilities both from the perspective of the certification and registration authorities and from the perspective of the users in terms of subscribers and partner entities.

The obligations and responsibilities set forth below are governed by mutual agreements established between the said parties on the basis of the applicable legislation.

2.1. Obligations

2.1.1. Obligations of the Certification Authority

By means of an assurance policy and made available to users, a certification authority assigns a number of fundamental obligations as follows:

- Document set up (in particular the Practice and Procedures Code) to define the way of working, general company politic, rights and responsibilities of the parties contracted to be approved by management and published in an accessible environment for the target.
- Carry out the activity in accordance with the procedures described in this Code of Practice and Procedures;
- Implementing reliable hardware and software resources to sustain the smooth running of the business on a permanent basis based on the regulations of the Certification Authorities, as well as in terms of the business environment;
- The processing of certificate issuance applications only through a Registration Authority with which there is a contractual association and which also operates in the manner established by this Code of Practice and Procedures;
- 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;

- Revocation of digital certificates if the data contained in the certificate is no longer up to date, if the private key corresponding to the certificate is compromised or if the user of the certificate has acted contrary to the regulations stipulated by this document. This situation requires the Certification Authority to notify the user of the measures taken;
- Ensure an infrastructure that allows the use of registration, issuance and entry into possession of certificates exclusively by electronic means;
- Creation and permanent management of a Certificate Registry Register issued by all Subordinate Primary Certification Authorities to allow access to information on issued certificates at any time.

2.1.2. Obligations of the Registration Authority

The Registration Authority defines its activity around the validation, approval or rejection of certificate applications by requesting the revocation of certificates and by approving renewal requests.

The Registration Authority is responsible for the information collected, which is why the security requirements imposed on the certification authorities are similar to those imposed on any registration authority.

Among the obligations of the Registration Authority are:

- Implementing reliable hardware and software resources to support the smooth running of your business on a permanent basis;
- Carry out the activity in accordance with the procedures described in this Code of Practice and Procedures;
- 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;
- Ensuring the correctness of user data that is validated and sent to the Certification Authority to be included in the certificate;
- Providing clients with the contracts to be signed to obtain a certificate;
- Use of the private keys of the operators only for the purposes stated in the Code of Practice and Procedures;

- Delivery of keys and / or certificates to subscribers;
- Protection of the PIN code and private key to be delivered to a subscriber against possible interceptions.

2.1.3. Obligations of the user

This document is an integral part of the contract between the Certification Services Provider and the user of the certificate. Thus, based on this agreement, the user expresses the consent of his / her integration into the certification system in accordance with the norms specified in this document and is subject to the following obligations:

- Subscription to contract terms;
- Subject to the rules and procedures described in this Code of Practice and Procedures;
- Know general information about certificates, electronic signatures and PKI.
- Obtaining public key certificates from certification and registration authorities;
- Providing valid data to certification and registration authorities. Users are required to understand the consequences that may result from the use of forged data;
- Acceptance of the electronic signature created by a private key and associated with an approved certificate containing a public key as its own signature and acknowledgment that the certificate was not invalid (out of date), revoked or suspended when creating the signature;
- Approval of the certificate that was issued to it. By this approval, the CertDigital guarantees and obligations are being applied to the user in connection with a certain type of certificate;
- Use of public key certificates and private keys only for the purposes defined by the certificate and in accordance with the areas of applicability and the restrictions established by the Code of Practice and Procedures
- Adopting the necessary measures to safely store the private key in a key pair;

- Notification of the issuer of the certificate when it finds the breach of security of the private keys or has suspicions about this fact;

2.2. Responsibilities

2.2.1. Liability of the Certification Authority

In accordance with the regulations on the liability of certification service providers under Law no. 455/2001 regarding the electronic signature, CertDigital, as a Certification Service Provider, who issues certificates presented as being qualified or who guarantees such certificates, is liable for the prejudice to any person who bases its conduct on the legal effects of the respective certificates (art. 41 of Law 455/2001 on Electronic Signature):

- As to the accuracy, when issuing the certificate, of all the information contained;
- As regards the assurance that at the time the certificate was issued, the signatory identified in it contained the signature-generating data corresponding to the signature verification data specified in that certificate;
- As regards ensuring that signature-generating data correspond to signature verification data, if the certification service provider generates both;
- With regard to the suspension or revocation of the certificate, in cases and subject to the conditions stipulated in art. 24 par. (1) and (2);
- As regards the fulfillment of all the obligations stipulated in art. 13-17 and art. 19-22, unless the Certification Service Provider proves that, although he did the necessary diligence, he could not prevent the injury.

Upon receipt of the application for issuance of the certificate, the supplier concerned shall verify, before issuing the certificate, the following aspects (Article 24 of Law 455/2001 on Electronic Signature):

- If the applicant for the certificate is the person identified in the application, by the appropriate procedure for the category to which the certificate belongs;
- If the applicant for the certificate holds the private key corresponding to the public key listed in the certificate;
- If the information listed in the certificate is accurate.

Based on art. 42 under the same law, the certification service provider may indicate in the contents of a qualified certificate restrictions on its use and limitations of the value of the operations for which it may be used, provided that such restrictions may be known by third parties.

The Certification Service Provider will not be liable for damages resulting from the use of a Qualified Certificate in breach of the restrictions contained therein.

CertDigital has adequate financial, material, technical and human resources to guarantee the security, reliability and continuity of the certification services offered.

Thus, CertDigital has concluded a Third Party Liability Insurance Policy in accordance with the requirements of Law 455/2001, which guarantees the payment to third parties of any damages incurred as a result of carrying out the activity of providing qualified certification services. The values of the dispatch comply with the requirements of the aforementioned law and its methodological norms.

From a technical point of view, CertDigital has taken all the measures in force in the field of electronic signature to guarantee to its customers the continuity of the certification services as well as the restriction of the unauthorized access to the data managed by the computer systems used. These measures correspond to best practices in the field of information security, defined in Standards such as ISO 27001, COBIT or ITIL.

From the point of view of the human resources used, CertDigital has staff with experience in the field of information security and electronic signatures.

2.2.2. Liability of the Registration Authority

The Registration Authority holds strict responsibility for the issues that relate to the subject matter of its activity.

The relationship between the user and the certificate issuing authorities regarding the guarantees and limits of liability between the parties is subject to and is governed by the Agreements Agreed and applicable Legislation.

2.2.3. Liability of users

The issues mentioned in Chapter 2.1.3 on User Obligations and Warranties constitute the legal basis for users' liability. The Digital Certificate Supply

Agreement concluded between the customer and CertDigital includes the circumstances in which this liability occurs.

The Certification Services Provider CertDigital will claim damages for customers in violation of the provisions of this Code of Practice and Procedures as follow:

- Provide false information for issuing the certificate;
- Using a name that significantly contravenes the intellectual property rights of a third party;
- Ignoring security measures on the private key resulting in the loss, compromise or unauthorized use of the private key;

2.3. Interpretation and application

2.3.1. Applicable law

The provisions and activities carried out under this document will comply with the provisions of the Romanian legislation in force in the field of certification services.

The regulations for the provision of certification services for qualified certificates are in particular defined in Law no. 455/2001 on electronic signature.

2.3.2. Entry into force

Entry into force of the Code of Practice and Procedures is made on the date of notification to the Regulatory and Supervisory Authority and is valid until the date of issue of a new version.

2.3.3. Applicability

The rules specified in this Code of Practice and Procedures are applicable to the issuance of certificates on the basis of the obligations mentioned in Chapter 2.1 and to users when concluding a contract in accordance with the provisions of this document.

2.4. Fees

2.4.1. Fees for the issuance or extension of a certificate of dormancy

CertDigital services are provided with a cost, and the exact rates are set according to the nature and complexity of the services offered.

2.4.2. Fees for related services

CertDigital reserves the right to charge additional tariffs for services provided (egg implementation services, consultancy, training, etc.) if they are subject to the agreement between the parties.

2.5. Publishing and storing information

2.5.1. Publication of information by CertDigital

For publishing public interest information, CertDigital implements a dedicated interface accessible at ca.certdigital.ro, which includes the following types of information:

- CertDigital Code of Practice and Procedures (version in force and previous version);
- Confidentiality statement for processing and storing personal information;
- Audit reports;
- Issued certificates;
- List of revoked certificates.

2.5.2. Frequency of publications

Publishing updates for the above information is done as follows:

- Code of Practice and Procedures - is published in accordance with the provisions of Chapter 7 ("Document Management");
- Audit reports - along with their delivery by the auditor;
- Issued certificates - are published immediately after issue;
- List of revoked certificates - is published after each revocation of a certificate within a maximum of one day.

2.5.3. Access to published information

All information published by CertDigital through the online interface is public and no special rights are required for viewing.

To prevent unauthorized access to the information storage, CertDigital has implemented a number of logical and physical measures that protect against the addition, modification, or deletion of published information.

2.6. Compliance audit

CertDigital outsourced IT auditing services to enhance maximum security and compliance with documented policies and practices.

As a result of the audit process, CertDigital aims to obtain additional risk management reviews.

The external audit of CertDigital's compliance with CertDigital policies and procedures is supported by a public entity independent of CertDigital, which has auditors of computer systems certified by ISACA (Association for Audit and Control of Information Systems)

2.7. 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.

Access to Qualified Certificates can only be obtained if the certificate holder has agreed to publish the certificate.

The use and processing of personal data by CertDigital is carried out strictly to the extent that this activity is required to issue a qualified certificate.

CertDigital provides all protection against unauthorized access to personal and organization-related data not included in the certificate, including during the signature-creation process.

2.8. 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.

3. Certificate management procedures

Obtaining a qualified digital certificate is done in several stages, each stage having a well-defined role and being carried out under the responsibility of the applicant, the Registration Authority or the Certification Authority.

3.1. Request a certificate

If an entity wishes to obtain a digital certificate, it must submit a request to CertDigital following the procedure described in this Code of Practice and Procedures. These requests are processed by the CertDigital Certification Authority and, as the case may be, are approved or not.

Key generation takes place in a secure environment and can be done by the Certification Authority, the Registration Authority or by the signatory. To generate the keys, secure and approved devices are used for the purpose of creating electronic signatures. The functionality of these devices does not include the export of privately generated keys.

In connection with obtaining a certificate, the client will enter into an agreement with CertDigital that includes an agreement to make known the obligations the client has, an agreement on the publication of the certificate issued to the CertDigital depositor and a statement on the truthfulness of the information provided.

CertDigital also provides the customer with the confidentiality statement that ensures the protection of personal information.

The process of registering a user is based on policies and procedures by which the Certification Authority obtains all necessary data to identify an entity before issuing a qualified certificate.

User registration is done only once, and will be included on the list of authorized users after pre-checking the provided data.

Recording customer data is the point of entry into the system and has the role of registering a qualified certificate application. Two categories of information are received in this process:

- Information about the applicant and the required certificate;
- Documents required for the issue of the qualified certificate.

The registration authority has the obligation to make copies of the original documents received from the applicant and to keep them on the basis of the methodology of archiving personal information. These methodologies are defined in the internal procedures for the protection of personal information.

Within the web form, information is requested in several steps about the applicant, the institution he represents and the certificate.

- **Step 1**: - Enter the CNP of the client, or for non-Romanian citizens, enter the unique identification code. Depending on this code, the system will check whether the client is in the database or is a new client. Depending on this check, go to the next step.
- **Step 2**: If the customer is a new user of CertDigital certification services, then in this step you will need to complete all your personal data (name, surname, address, serial and ID number, other contact information etc.). If the client is already in the database, then he will be required to update those fields, if applicable.
- **Step 3** The information related to the certificate to be issued is entered: the e-mail address, the institution, the function and optionally the location and address of the client. During this step, through a Java signed applet, DCSC (Secured device for electronic signature creation) is being accessed and it needs to be connected to the computer. The DSCS will generate a pair of keys that will be related to the certificate to be issued. The public key is packaged in a PKCS # 10 object and is sent with the other information to the Certification Authority server where it is stored in the database.

A client cannot have more than one valid certificate on the same email address. Once this information is complete, the user is notified that they will receive an email with the positive or negative response of the data validation.

For this registration step, a certificate request will be generated, which will wait for a data validator to accept or deny it. This response must be given within 24 hours.

The validation of the data is done after the copies of the documents originally submitted by the client to the Registration Authority or based on copies authenticated by a notary public are sent by post.

The documents required for issuing a certificate are:

- Identity card (identity card, passport);

- Declaration of responsibility by which the applicant expresses its agreement to CertDigital's general terms and conditions regarding the provision of certification services. The form of this statement can be downloaded from the CertDigital site.
- In case of certificates issued to institutions, a power of attorney or proof that the applicant is entitled to sign on behalf of the institution.

3.1.1. Name Types

Each entity must define a Distinct Name in the subject field of the certificate in accordance with the X509 V3.

3.1.2. Using pseudonyms

In accordance with Law no. 455/2001 on electronic signature, CertDigital certificates allow the use of pseudonyms as an alternative to the name by filling in an additional field in the registration form.

3.1.3. The need to use a name with meaning

The name corresponding to the subject in the certificate must represent the user of the certificate in a simple way and must have a reasonable association with the real name of the authenticated user.

3.1.4. Uniqueness of names

The Distinct name must be unique for each subject certified by the Certification Authority CertDigital. If the name presented by the subscriber is not unique, numbers and additional letters are added to the common name to ensure uniqueness.

Users can not alienate the certificates they have been granted.

3.1.5. Procedure for resolving disputes arising out of the use of the name

CertDigital Certified Applicants are forbidden to use names that violate intellectual property rights. CertDigital does not verify if a certificate applicant holds intellectual property rights for the name entered on the request and is not responsible for resolving disputes arising out of that claim.

CertDigital is entitled to reject or suspend a subscriber's request for conflicts without assuming any responsibility in this respect.

3.2. Issuing a certificate

The information provided by the applicant through the request for issuance of the certificate is processed by CertDigital in accordance with the provisions of this document.

This processing is done by a person responsible for validating certificate requests. Validation or refusal to qualify for the Qualified Certificate is made using the same web application described in the registration step, only that person has a special account that gives him increased entitlements to an ordinary client.

Also, at this stage, the payment of certification services is verified, which the applicant has to do using any legally accepted payment method.

If the results of these processes are validated by the authentication conditions, CertDigital approves the request for certificates, respectively rejects it if nonconformities are identified.

If the request has been validated, the system will send an email to the requester, which will contain a URL to a page from where the certificate issued can be downloaded.

3.3. Shelf life and certificate format

The period of validity of the Qualified Certificates issued by CertDigital is one year from the date of issue in accordance with Law no. 455/2001 regarding the electronic signature, and the format complies with the X509 standard V.3.

3.4. Electronic register of issued certificates

CertDigital permanently maintains an Electronic Register that highlights the issued certificates and can view certificate information:

- the exact date and time at which the certificate was issued;
- the exact date and time when the certificate expires;

- Where applicable, the exact date and time at which the certificate was suspended or revoked, including the causes that led to the suspension or revocation.

The Electronic Certificate Record is always available for consultation via the CertDigital website.

3.5. Acceptance of the certificate

CertDigital will send the confirmation of issuing the certificate to the users together with the entry procedures.

Downloading the qualified certificate is done by the certificate applicant and it is necessary that the Secure Device to create the electronic signature be connected to the computer from which these actions are carried out.

This activity is carried out via an Internet connection and requires the use of a secure connection on the HTTPS protocol imposed by the CertDigital server.

Users are required to verify the contents of the certificate upon receipt of the certificate, in particular the correctness of the data and the complementarity of the public key with the private key it owns, and to notify CertDigital of any error in this respect. In such situations, CertDigital undertakes to cancel the issued certificate and ensure the re-issuance of a new certificate.

After a period of 7 days from receipt, the issued certificates are considered validated by the users.

Based on the user-approved agreement at the time of requesting the certificate, CertDigital will publish any new certificate issued in the information warehouse.

Once the certificate is accepted, the user accepts the rules of this Code of Practice and Procedures and is subject to the use of the certificate in accordance with the required conditions.

The Registration Authority stores the copies of the documents and statements submitted by the clients when issuing the certificates. Also, the Registration Authority keeps printed versions of qualified certificates issued.

Existing certificates in the database can be viewed using the search application's certification feature.

3.6. Revocation of a certificate

The user of a certificate can revoke the functional capabilities of the certificate if the private key is compromised in an irremediable form or if the information in the certificate no longer corresponds to reality.

The revocation process may be requested by the user or by a person who has revocation rights if the Certification Authority, CertDigital, considers that revocation of the certificate is required under the Electronic Signature Law.

Based on the password introduced in the Qualified Certificate Issuance process, a user can access a specific email address to which they can revoke the certificate by entering the email address and password associated with that certificate.

If the user has forgotten the password or does not have Internet services, he / she will be able to ask Certification Authorities to revoke the certificate. This request will need to be accompanied by a legitimation of the user's identity, who will have to prove that he is the owner of the certificate that is being revoked.

A revocation of the certificate may also take place after a self-certification by the Certification Authority or at the request of certain state authorities under the Electronic Signature Law.

Revocation of a certificate does not affect the transactions made prior to revocation or the obligations resulting from compliance with this Code of Practice and Procedures.

When revoked, the certificate is included in the List of Canceled Certificates of the Electronic Certificate Registry and is considered invalid. Registration of certificate revocation is made immediately after the revocation request is registered.

3.6.1. Circumstances for revocation

Revocation of a certificate is made when:

- A request for revocation was issued by the signatory or an authorized entity;
- The agreement between the parties has expired;
- CertDigital ceases to provide these services;
- The information provided by the signatory in the issuing request is false;
- The user's private key is irreparably compromised;

- CertDigital decides that the issue of the certificate has not been performed in accordance with the procedures required by the Code of Practice and Procedures;
- CertDigital discovers that the certificate was issued to someone other than the one mentioned in the certificate without its authorization;

3.6.2. Procedure for revocation request

The request for revocation may be filed as follows:

- The Signatory or an Authorized Entity requests the revocation of a certificate by a completed and handwritten cancellation form at the CertDigital Certification Authority.
- The Signatory or Authorized Entity requests the revocation of a certificate by an electronic revocation request to CertDigital. In this case, the authentication of the revocation is provided by a qualified electronic signature.
- Online services made available by CertDigital.

3.6.3. Procedure for Suspension Application

CertDigital does not offer the possibility to suspend the issued certificates.

3.7. Extend the validity for a valid certificate

The process of renewing a certificate and, implicitly, extending the period of validity implies the existence of a valid certificate and a corresponding private key.

By renewing, CertDigital will issue a certificate with the same public key whose information is taken from the previous certificate but with the change of the serial number, issuer's signature and the validity period.

3.8. Modifying a valid certificate

If the user requests the issuance of a new certificate due to the modification of some of the existing information, CertDigital will issue based on the existing certificate (if it is valid) a new certificate with a new public key and a new serial number. Issuance of the new certificate is made after previously verified and confirmed information that has undergone changes.

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, 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.

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 driving a key, devices that only the system administrator and the CEO can act on.

4.1.3. Protection of private keys and qualified certificates

The storage of private keys used to issue certificates is done by secured equipment that is certified to comply with the provisions of Law no. 455/2001 on electronic signature and can not be falsified. To prevent any unauthorized access or tampering of sensitive information, CertDigital implements appropriate, periodically reviewed controls to ensure proper operation.

Qualified certificates are stored on reliable systems that allow only authorized persons to enter and modify certificate information.

Third-party certificates can only be consulted if their owner agrees;

Moreover, the CertDigital systems track every technical change that could jeopardize the implemented security systems. This track is being permanently monitored by authorized personnel of CertDigital.

4.1.4. 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 for the areas that the responsible manager has marked as restricted areas;
- Access rights for collaborators, consultants, cleaning staff, etc. Is allowed only in the areas in which it operates. Access will be made by specifying the place and time required and will be approved by the responsible manager;
- Visitors are only allowed 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.

4.1.5. 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;
- 4 UPSs each with 1000W power. These UPSs are connected to the four servers, the HSM, the router, the firewall, the internet switches and modems;
- Connection to a separate electrical grid to provide protection against overvoltage;
- To avoid possible threats (such as floods), the equipment in the dedicated Certification Authorities room 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, which ensure the performance of qualified certificates issuance in optimal conditions:

- 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 Mirroring matrices made up of two 500GB SATA disks - capacity for each server. Data duplication provides protection against physical loss of information.

Clustering system for the Certification Authority

The Certification Authority Server (ca.certdigital.ro) is set to work in clustering with another backup server, thus ensuring a high level of availability of services.

Systematic backup process

The data on the ca.certdigital.ro server as well as the information on HSM are 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 the continuity of the services offered, the Certification Authority 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. Measures to protect employees from mistakes

Qualified staff in certification activities

CertDigital Certified Authorizing Officer staff is made up of highly qualified and highly trained people with certifications and diplomas.

Qualified and experienced staff

Personnel nominated to be part of the certification team must provide evidence of past experience, qualifications and experience required to perform competently and satisfactorily the job responsibilities.

Segregation of activities

Activities are rooted according to the responsibility sheet, so that a more complex activity can only be done with the consent of several 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 General Director is required.

Another example is issuing Qualified Certificates, where we are responsible for entering data, responsible for validating them, who can revoke certificates, or administrators who can create new user accounts and change their roles.

4.3. Data rescue and restoration procedure

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

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

4.3.1. The rescue process

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

- The SQL Server database, where all the issued certificates are kept, and information about them: the recipient, the date of issue, the validity, etc..
- Key pairs and certificates of all authorities in the CertDigital Trusted Tree. This information 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** - is run 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. The save is performed on the Network Storage in a file named “ca_full_backup.bak”.
2. **Differential Back-up -** Is executed automatically once a day, at 1.00 pm and consists of saving all database changes 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 "as log_backup.bak".

Back-up of key pairs and certificates is executed whenever the structure of CertDigital certification authorities changes, or automatically, programmatically, every 1 and 15 days of each calendar month.

Saving HSM data will be done using the HSM client application installed on "ca.certdigital.ro". The HSM backup file is encrypted, and can only be used for the data restoration process.

The files will be saved with the * .backup extension and will be stored on the NetworkStorage in the BackupHSM \ YYYY.MM.DD location hh: mm, where YYYY.MM.DD hh: mm represents the Year.Month.Day Time: Current Minute.

Every Friday on weekdays, Network Storage saved on both the SQL database and the HSM certificates' savings are written on CD / DVD magnetic media, which will indicate the date and time at which they were saved. Subsequently, the CD / DVD drives are kept in a safe place in key-protected metal lockers and dedicated security system within CertDigital.

4.3.2. Restoration procedure

The implementation of restoration procedures is carried out as follows:

- The IT department performs at least quarterly backup environment testing 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 detected, 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.

4.4. 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 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 may create confusion, etc.).

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

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. Create 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 immediate 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 liquidation letter.

In order to facilitate the traceability of activities performed with user accounts, these 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 to 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, debugging, etc.).

The privileged rights are identified for each element of the infrastructure (egg 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 respective envelop.

4.5.1. Managing user accounts with privileged rights

Application management personnel have the responsibility to create, modify, and delete 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 staff

The purpose of this procedure is to establish 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 within CertDigital applications or various systems (e.g., 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 lower case letters (a-z, A-Z);
- Include 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:
  - he 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 accounts, etc.). Also, passwords are chosen distinctly for each type of application that requires password authentication.

All passwords are classified as confidential information and are not allowed to store them in computer systems or on another medium.

If checks on the use of passwords are not being met, CertDigital takes appropriate steps to comply with them.

4.7. Usage procedure for electronic mail

To increase performance, the CertDigital Certification Authority favors the use of electronic communication (Internet, phone, pager, voice, e-mail and fax).

All messages emitted/handled through CertDigital electronic systems are considered to be the property of that person except in situations where third parties expressly express their copyright or other rights of this kind over electronic messages that have passed through the previously announced electronic systems.

Managing the email system is only done by employees of the IT Department.

The administration of email boxes will be done taking into account the internal procedures of the Company.

4.7.1. Rules on the use of email

The use of the CertDigital electronic messaging system should be carried out as part of the professional activity that aims to improve daily activities by facilitating internal communication within CertDigital and externally by maintaining links with customers, CertDigital business partners or local authorities.

Electronic communication will be limited to materials related to professional activities and employee service tasks and will not be used as support for charitable fundraising campaigns, political / religious support campaigns or for personal business activities, amusement Or distraction.

This procedure prohibits the use of public e-mail systems for sending messages about CertDigital activities.

It is forbidden for a user to use an email address belonging to another person.

In formulating electronic messages, the user is required to specify identification data that must reflect his or her name, telephone number, e-mail address, or membership of a particular organization (except "hot-line" lines that are , generally anonymous). It is also recommended to attach an electronic signature within the messages containing information about the sender, such as: the position occupied within CertDigital, its affiliation, address, etc.

Periodically, employees are informed and trained to adequately use the resources of the Company's IT system.

In the electronic communication, it is forbidden to replace, remove or distort the identity of a user.

4.7.2. Rules about message content

Use of pejorative remarks or obscene speech in e-mail discussions with other employees, customers, competitors or other people is strictly forbidden, as they may be the basis of legal issues that could cause defamation of CertDigital. These remarks can then be detached from the original context and used against CertDigital. Under these circumstances, in order to avoid such problems, employees will have to confine themselves to electronic communications only to communicating CertDigital business issues in accordance with conventional standards of ethics and goodwill.

4.8. 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 in internal computer systems that could damage the CertDigital image.

CertDigital uses three categories of information classification detailed below.

4.8.1. 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.

4.8.2. Internally used information

The use of this information is allowed within CertDigital, and in some situations and within affiliated organizations (CertDigital partners). Unauthorized disclosure of this type of information to people outside of CertDigital is not permitted and can cause problems within your 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).

4.8.3. 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 who are unnecessary may constitute a violation of applicable laws and regulations and may cause problems for the organization, clients 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).

4.9. Personnel procedure

4.9.1. Past experience, qualifications, experience and acceptance

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

4.9.2. Procedures for checking the past

CertDigital makes the following checks on the past of staff who will handle the issue / revocation of Qualified Certificates and Trademarks:

- Confirmation of your previous job;
- Check 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;
- Search for social assistance reports;

To the extent that any of the imposed requirements cannot be satisfied, CertDigital will use an investigative technique that is permitted by law and which 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:

- The wrong presentation made by the candidate;
- Personal or unfavorable personal references;

- Sentences;
- Indices of lack of financial responsibility.

Reports containing such information are evaluated by human resources and security staff, which determine the appropriate course of action, depending on the type, importance and frequency of behavior revealed by past verification. 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.

4.9.3. 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;
- Using and running existing hardware and software;
- Reporting and handling incident and compromise cases;
- Disaster Recovery and Business Continuity Recovery Procedures.

4.9.4. Requirements and frequency of training courses

CertDigital provides training and upgrading for staff, to the extent and frequency, to ensure that the level required to meet the competence and satisfactory performance of the service is maintained. Periodic security training is provided.

4.9.5. 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 termination of the contract and are taken in accordance with the frequency and severity of the actions.

4.9.6. 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.

4.9.7. 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 the Internal Security Policy. CertDigital offers its employees the necessary training and other documentation to fulfill competently and satisfactorily the responsibilities of the function.

5. Information security controls

5.1. Generate and use the key pair

5.1.1. Generate the key pair

The process of generating key pairs within the CertDigital Certification Authority is performed by trusted people using trustworthy systems and processes that include key security and cryptographic structure within key pairs.

The cryptographic hardware system used to generate key pairs meets the requirements of FIPS 140-1 Level 3.

All key generation activities are recorded, dated and signed by all persons involved. Supporting documents related to key generation processes and other sensitive operations are stored and made available to auditors for further review.

5.1.2. The hash and encryption procedures used

In accordance with Article 39 of the Technical and Methodological Norms for the Application of Law no. 455/2001 on electronic signature, the Certification Authority CertDigital only uses the SHA-1 hash-code function and the RSA encryption algorithm.

5.1.3. Private Key delivery

If a user's keys were generated by the Certification Authority, delivery to the user is done in two ways

- Shipped personally by storing on a cryptographic device (for example, token), or in some cases in PKCS # 1 format;
- By recommended postal letter

The information required for key decryption or activation of the card (PIN code) or (password) is provided separately from the storage medium containing the key pairs.

5.1.4. Delivery of the public key to the issuer of the certificate

The signer sends the public key generated by an electronic request to an issuer in an SSL secure session that complies with the standard syntax for PKCS # 10 certificate applications.

The delivery of the public key takes place in the same session with the submission of the details by the applicant in the application for the certificate issuance.

5.1.5. Public key delivery to users

In accordance with X.509 Version 3, CertDigital distributes public keys in the form of certificates through e-mail services or the CertDigital site by downloading.

5.1.6. Key dimensions

The CertDigital Certification Authority key pairs are 2048 bits defined, and those for users defined are 1024 bits.

5.1.7. Generating the hardware / software key

The key pairs of the subscribers are generated and stored in the hardware and software infrastructure. It is recommended that subscribers use a FIPS 140-1 cryptographic module for key generation.

5.2. 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 Certification Authority are generated and stored in hardware security modules (HSMs) that can be activated simultaneously by only two people, and which is also validated by FIPS 140-1 Level 3.

Depending on the state in which it is located, a key (public or private) can be assigned to one of the following phases:

- "Waiting" - the key is generated, but it is not released during the validity period;
- "Activate" - the key is fully usable in terms of functionality;

- "Expired" - the validity period of the key is exceeded. The key can only be used to validate electronic signatures, not for creation.

5.2.2. Multi-person control 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 can not be accessed without the information held by authorized persons.

5.2.3. Private Key back-up

CertDigital private keys are generated and stored in a cryptographic hardware module. If these keys are to be transferred to other environments for backup purposes, they are transferred and stored in encrypted form on specialized key storage equipment.

All private key back-up processes are performed in accordance with the controls described in section 6.1.1.

5.2.4. Archiving private keys

The Certification Authority CertDigital does not normally store copies of the private keys of the certificate users. Creating these copies is done only at the request of users..

5.2.5. Enter a private key in the crypt module

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

Transferring private keys to the outside is done only in encrypted forms.

5.2.6. Activate private keys

Enable private keys for CertDigital Qualified Qualified Certificates 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.

5.2.7. 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.

5.2.8. 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.

5.2.9. The format of documents that can be signed electronically

The certification services provided by CertDigital allow the use of the signature for any type of electronic document.

For example, if the document to be signed is a PDF format, then it will also result in a PDF format, which has an XML structure that allows for the inclusion of electronic signatures in the file.

For any other file, a tire file will be generated, including the old file and the signatures. This file will have the P7M extension (PKCS # 7 Message).

5.3. Other aspects of key pair management

5.3.1. Archiving public keys

CertDigital certificates issued to users are stored in the certificate repository and on backup media.

5.3.2. Period of use of private and public keys

Certificates issued by CertDigital and the corresponding key pairs can be used for the entire validity period if there are no violations of regulations requiring immediate revocation.

n the case of private and public keys, the expiration of the validity period determines the downgrading of the decryption functionality (in the case of private keys), the respect of signature verification in the case of public keys.

The validity of CertDigital certificates is structured as follows:

Certificate issued by:	**Validity:**
ROOT Certification Authority	25 years
Sub-Authorities	10 years
Certification authority for users	1 year

In the event of litigation, in order to prove certification, the information on a qualified certificate is kept for a minimum of 10 years from the date of expiry of the certificate's validity.

5.4. Activation data

5.4.1. Installing and generating activation data

To enable hardware security, CertDigital staff and service users are instructed to use strong authentication passwords.

Through an appropriate policy, CertDigital employees establish passwords in accordance with the password management procedure described in this document.

5.4.2. Protection of activation data

Activation data for hardware security modules is protected as specified in section 6.2.2.

CertDigital employees are instructed not to disclose foreigners' passwords and not to write passwords on environments that might be accessible to others.

5.5. Security checks of the computing stations

CertDigital's servers and computing devices run on trustworthy systems configured and tested using industry best practices. All operating systems require individual identification and access control restrictions on authentication-based authentication services

Systems are scanned for malware detection, and are also protected against spyware or viruses.

The CertDigital network is provided with firewall solutions to protect against intrusion attempts from inside or outside and to limit network processes that could cause vulnerabilities in production systems.

5.6. Life Cycle Technical Controls

5.6.1. System-specific controls

The implementation of CertDigital systems is done in accordance with current standards on system development and change management.

Before they are released in the production environment, the results of implementing the changes are tested in a test environment.

The testing process is carried out by IT staff and end-user representatives of applications in departments using the system that has been modified.

Testing is based on predefined test scenarios, which include among other things the persons responsible for testing, the duration of the tests, the test data, etc.

If applicable, the following types of tests will be performed:

- Functional testing;
- Integration tests;
- User Acceptance Testing - ATU

Test data will not be used in the production environment, and production environment data will be used for testing unless it has been depersonalized.

5.6.2. Security management controls

CertDigital implements security management controls to ensure optimal functionality of IT systems and implicitly to guarantee operation in accordance with operational requirements.

CertDigital has implemented within IT systems controls that enable permanent verification of the integrity and availability of systems in hardware and software.

5.7. Network security controls

CertDigital IT Infrastructure benefits from both internal and external protection systems through the use of firewall solutions and intrusion detection systems.

User access to CertDigital systems is only allowed directly for processes that have a close connection with the activity they perform.

6. Certificate Profiles and Certificate Revocation List

6.1. Certificate profiles

Certificate profiles issued by CertDigital comply with X.509 standard 3.

According to this standard, the structure of a certificate consists of:

- the body of the certificate;
- information about the algorithm used for signing the certificate;
- proper signature of the Certification Authority.

6.1.1. Content

The base fields of a CertDigital certificate are:

Field	Required value or value
Version	X.509 Version 3
Serial number	Unique value for CertDigital certificates issued
Signature algorithm	Object identifier of the algorithm used to sign the certificate (SHA-1 hash-code function and RSA encryption algorithm)
ND Issuer	Authority issuing the certificate
Valid starting with	Date of Certificate Validity Validation Start Date Based on Server Synchronization with the Official Time of Romania
Valid until	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 (Name Distinct)	The distinctive name meets the requirements of the X.501 standard. Certain attributes in the Distinct Name component may be optional.
The subject of the public key	Coded according to RFC 3280

Signature	Generated and encoded in accordance with RFC 3280

6.1.2. Version number

CertDigital Certification Authority and end-user certificates are issued certificates complying with X.509 standard 3.

6.1.3. Extensions

In according to the X.509 standard version 3, the certificates issued by VertDigital include the following extension fields:

Extension field	Meaning
basicConstraints	Critical Extension with False Value
keyUsage	Critical Extension with digital Signature, **keyEncipherment**
subjectAltName	Non-critical extension attaching an additional identity to the subject of the certificate (for example, an email address)
authorityKeyIdentifier	Non-critical extension that identifies the certificate of the Certification Authority required to verify an issued certificate
qcStatements	Non-critical extension indicating that the certificate issued is a qualified certificate

6.1.4. Signature algorithm identifier

The identifier specified by the Signature Algorithm field refers to the cryptographic algorithm used for the electronic signature of the certificate. In accordance with Article 39 of the Technical and Methodological Norms for the Application of Law no. 455/2001 on electronic signature, the Certification Authority CertDigital only uses the SHA-1 hash-code function and the RSA encryption algorithm.

6.1.5. Field specifying the electronic signature

Field value signature is obtained by applying the hash function to the certificate fields.

6.2. Revocation Certificate Profile

Lists of revoked certificates comply with X.509 standard 3.

In accordance with this standard, the structure of a list consists of three types of information as follows:

- information about revoked certificates;
- information about the algorithm identifier used to sign the list;
- information about the electronic signature of the Certification Authority.

6.2.1. Content

The base fields of a revoked certificate list are:

Field	Required value or value
Version	See section 7.1.1
Certificate Revocation List number	Number assigned to revocation certificate list versions
Issuer	Authority that has signed and issued the List of Canceled Certificates
Date of entry into force	Date on which a Certificate Revocation List was issued. The vigor is done after the issue
Signature algorithm	Object identifier of the algorithm used to sign the Certificate Revocation List (SHA-1 hash-code function and RSA encryption algorithm)
Date of the next update	Date of issue of the next Certificate Revocation List
Certificate revoked	List of revoked certificates, including the serial number of revoked certificates and the date they were revoked.

6.2.2. Version number

Evocated Certificate Lists issued by CertDigital comply with X.509 standard 2

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.

The implementation of the changes updates the version number of the document and the date of issuing the Code of Practice and Procedures, depending on the date the changes were made.

Authorized Certification 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 Code of Practice and Procedures.

Revisions to the Code of Procedures and Practices with no impact or insignificant impact on Signatory and Trusted Parties using CertDigital Certificates and related Certificate Status information can be made and recorded without notifying users and trusted parties and not involving the change of version number of the document or the date of entry into force.

Changes that require notifications to entities include:

- Changes made to the extension for a group of certificate users;
- Inclusion of new types of certificates;
- Significant changes in content and interpretation of Certificate fields and Certificate Revocation List.

Along with the synthesis of the changes to be implemented, the Code of Practice and Procedures enters into an internal approval procedure based on a committee consisting of the Director-General, the Deputy General Manager and the Managers of the Technical Departments.

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

The current version of the Code of Practice and Procedures is dated March 2011.

7.2. The mechanism of publication and notification

The Code of Practice and Procedures Code is available electronically on the CertDigital site at: ca.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.

7.3. Procedure for approving the 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 Code of Practice and Procedures and related changes are required within 15 days of the validation of the new version to make a statement to that effect. In this case, the CertDigital Certification Authority assigns the right to terminate the contract for the provision of certification services and the revocation of the certificate issued on its basis. Subsequent to the 15 day period since the new version came into force, CertDigital considers user acceptance implicit.