Certification Practice Statement

DigiSign Certification Authority

Qualified Electronic Certificates

compliant with eIDAS Regulation and national legislation

Category:	**Public Document**	Language:	**English**
Written by:	**Policies and Procedures Management Body**		
Verified by:	**Internal Auditor**	Edition:	**5**
Approved by:	**General Manager**	Version:	**2**

OID: **1.3.6.1.4.1.34285.1.1.1.2.3.1.0**

DIGISIGN S.A.

74B Nicolae G. Caranfil street, 1st District

014146, Bucharest, Romania

+4 031 620 20 00

+4 031 620 20 80

office@digisign.ro

www.digisign.ro

Document history

Edition	Version	Description	Date	Author
1	0	First release: Certification Practice Statement for DigiSign Certification Authority, compliant with eIDAS Regulation and national legislation	May 15, 2017	Policies and Procedures Management Body
1	1	Updates as per the recommendations resulted after the audit	June 15, 2017	Policies and Procedures Management Body
1	2	Updating features for end user certificates	November 17, 2017	Policies and Procedures Management Body
1	3	Updating with new identity validation method and added new authorities	November 22, 2018	Policies and Procedures Management Body
2	0	Updating with new identity validation method	October 15, 2019	Policies and Procedures Management Body
2	1	Minor updates	July 28, 2020	Policies and Procedures Management Body
2	2	Minor updates	June 25, 2021	Policies and Procedures Management Body
2	3	Minor updates at identity validation process	September 24, 2021	Policies and Procedures Management Body
3	0	Minor updates	May 27, 2022	Policies and Procedures Management Body
3	1	Updates as a result of the audit	October 28, 2022	Policies and Procedures Management Body
3	2	Updates as a result of the audit	January 14, 2024	Policies and Procedures Management Body

3	3	Update delivery period	March 07, 2024	Policies and Procedures Management Body
4	0	Update identity validation	March 12, 2024	Policies and Procedures Management Body
4	1	Update delivery period	May 12, 2024	Policies and Procedures Management Body
4	2	Update DigiSign PKI Hierarchy	June 20, 2024	Policies and Procedures Management Body
4	3	Update ISO Certification	October 08, 2024	Policies and Procedures Management Body
5	0	Minor updates	October 23, 2024	Policies and Procedures Management Body
5	1	Address update	December 21, 2024	Policies and Procedures Management Body
5	2	Update Video identification process	March 26, 2025	Policies and Procedures Management Body

Table of Contents

1. Introduction

DIGISIGN S.A. (hereinafter DigiSign) operates a Public Key Infrastructure (hereinafter PKI) in order to provide trust services, such as Qualified Electronic Signatures, Qualified Electronic Seals and Qualified Electronic Time-Stamps. DigiSign PKI is currently using a Root Certification Authority which have intermediate Certificate Authorities, dedicated to a class or type of service it provides. Within a Certification Authority, there are several certificate profiles used in order to issue a specific type of certificate.

As a Certification Authority (hereinafter CA), DigiSign issues high quality and highly trusted digital certificates to entities including private and public companies and individuals, in accordance with the rules, principles and practices outlined in this document. In its role as a CA, DigiSign performs functions associated with public-key operations that include receiving requests, issuing, revoking, suspending and renewing digital certificates, as well as maintenance, issuance and publication of Certificate Revocation Lists (hereinafter CRLs) and Online Certificate Status Protocol (hereinafter OCSP), for users within DigiSign PKI.

DigiSign is a leading Qualified Trust Service Provider (hereinafter QTSP) which successfully provides trust services, such as Qualified Electronic Signatures, Qualified Electronic Seals and Qualified Electronic Time-Stamps, and acts as a Trusted Third Party (hereinafter TTP) when it comes to the creation and validation of those services.

1.1. Information regarding this document

1.1.1. Name and identification

This document represents a public statement of the practices followed by DigiSign as a Qualified Trust Service Provider in order to successfully issue, renew, suspend, revoke, validate and generally administrate digital certificates, and is therefore named DigiSign Certification Practice Statement (hereinafter CPS). Throughout this document, unless otherwise specified, the use of the term *CPS* refers to the present document. This CPS is structured in accordance with RFC 3647 and ETSI EN 319 401 standard.

DigiSign Certification Practice Statement presents the criteria established by DigiSign to provide qualified electronic trust services which enhance trust and confidence in electronic transactions. Also, this CPS presents the practices used by DigiSign in order to provide Qualified Trust Services, such as Qualified Electronic Signatures, Qualified Electronic Seals and Qualified Electronic Time-Stamps, in conformity with EU Regulation no. 910/2014 (hereinafter eIDAS), the Romanian national laws and other relevant standards. Furthermore, this document presents the practices used by DigiSign in order to achieve a specific security level, for which DigiSign achieved ISO/IEC 27001:2023 certification.

Thus, this CPS describes the following:

- principles, rules and practices regarding the certificate life cycle, as well as the operational controls,
- details of DigiSign's trustworthy systems and operations,
- details concerning legal, technical and other business matters, common to all certificate types (and, thus, policies),
- details regarding the compliance audit and other assessments,
- practices regarding the policies management,
- general provisions of the obligations, liabilities and warranties of all participants in the certification process,

- compliance with eIDAS, Romanian national laws and other relevant standards.

This CPS refers and encompasses DigiSign Certification Policy (hereinafter CP) which represents a *named set of rules and principles under which a digital certificate is issued to a particular community and/or class of application with common security requirements*. The purpose of the CP is to establish what a participant within DigiSign PKI must do and the applicability of a certificate according to its type. This CPP is updated annually or whenever a change occurs.

1.1.2. Publication and contact

This CPS is publicly available as follows:

- online on 24x7 basis by accessing www.digisign.ro or by request sent to office@digisign.ro
- printed, on request, sent to DigiSign's headquarters.

The present document is available in two languages: English (the original document) and Romanian. In the event of conflict between the original document written in English and the translated document in Romanian, the original document shall prevail.

The present document is administrated by the Policy Management Body within DigiSign, in accordance with Chapter 1.4 – CPS Management. Further information about DigiSign's policies and practices can be obtained by e-mail.

DigiSign's headquarters and contact information are:

Address: 74B Nicolae G. Caranfil street, 1st District, 014146, Bucharest, Romania
Website: www.digisign.ro
E-mail: office@digisign.ro
Telephone: +4 031 620 20 00
Fax: +4 031 620 20 80

1.2. Certification process overview

The main goal of DigiSign PKI is to provide in Romania, but also outside national borders, electronic trust services based on public key certificates. DigiSign provides to End Users the following certification services:

- Registration services – verifies the identity and if applicable, any specific attributes of the certificate Subject;
- Certificate Generation services – generates key pairs, as well as creates and signs certificates based on identity and other attributes verified by the registration services;
- Dissemination services – disseminates certificates to Subjects and, with the Subject's consent, makes the certificates available to Relying Parties;
- Revocation management services – processes requests and reports relating to revocation to determine the necessary action to be taken;
- Revocation status services – provides certificate revocation status information to Relying Parties;
- Subject device provision services – provides and checks secure cryptographic devices to Subjects.

In order to do so, DigiSign uses the present public statement as ground for its Certification Authorities functioning. Furthermore, this document can also be considered the ground for end user's trust in DigiSign PKI, as it describes the rules applied for the identification of the Subject, the issuance and

renewal of certificates, as well as the procedure used in case of Disaster Recovery or Business Continuity.

In the certification process there are several entities which have the status of PKI Participants, such as:

- Certification Authorities which are identified in the certificate's structure as the Issuer. The CAs private keys are used to sign certificates, the CAs always maintaining overall responsibility, ensuring the policy requirements are met.
- End Users which can be Subscribers, Subjects or Relying Parties.
- Other participants: the Repository, the Registration Authorities, the Validation Authorities, the Time-Stamping Authorities etc.

1.2.1. DigiSign PKI Hierarchy

DigiSign PKI architecture is divided into several levels, according to the certificate applicability, signing algorithm and the type of the circuit (closed or public).

Level 1 contains the root certificates that acts as a point of trust and, thus, every certification path must start with the proper ROOT CA certificate:

- DigiSign Root Certification Authority (public circuit)
- DIGISIGN PRODUCTION TRANSFOND ROOT CA (closed circuit)
- DIGISIGN TEST TRANSFOND ROOT CA (closed circuit)
- DIGISIGN TRANSFOND EBUSINESS ROOT CA (closed circuit)
- DIGISIGN BNR PRODUCTION CA (closed circuit)
- DIGISIGN BNR TEST CA (closed circuit)

This Root CAs operates exclusively offline and are used to sign directly the Intermediate CAs from Level 2 and their own Certificate Revocation Lists (hereinafter CRLs). If Level 2 Intermediate CAs are compromised, the Root CAs are used to revoke those certificates and issue new ones.

Level 2 contains the intermediate certificates which are directly signed by the root CAs:

DigiSign Root Certification Authority signs:

- DigiSign Qualified Class 3 CA 2017 (public circuit)

DIGISIGN PRODUCTION TRANSFOND ROOT CA signs:

- DigiSign Production Transfond Qualified DS CA (closed circuit)
- DigiSign Production Transfond Simple SSL CA (closed circuit)

DIGISIGN TEST TRANSFOND ROOT CA signs:

- DigiSign Test Transfond Qualified DS CA (closed circuit)
- DigiSign Test Transfond Simple SSL CA (closed circuit)

DIGISIGN TRANSFOND EBUSINESS ROOT CA signs:

- DIGISIGN TRANSFOND EBUSINESS QUALIFIED DS CA (closed circuit)
- DIGISIGN TRANSFOND EBUSINESS SIMPLE SSL CA (closed circuit)

DIGISIGN BNR PRODUCTION CA signs:

- DigiSign for BNR Qualified DS Production CA V2(closed circuit)
- DigiSign for BNR Simple SSL Production CA V2(closed circuit)

DIGISIGN BNR TEST CA signs:

- DigiSign for BNR Qualified DS Test CA V2(closed circuit)
- DigiSign for BNR Simple SSL Test CA V2(closed circuit)

Level 3 contains the End Users certificates, issued and signed by the Intermediate CAs. The End Users certificates are described in the chapter which concerns their usage and applicability.

The certificates issued by DigiSign for Transfond CAs, can't be used in public hierarchy, their intended purpose being for the SENT and EBusiness systems, operated by TRANSFOND S.A. based on a technical protocol. This protocol is confidential and shall not be made publicly available.

The certificates issued by DigiSign for BNR CAs, can't be used in public hierarchy, their intended purpose being for the ReGIS and SaFIR systems, operated by National Bank of Romania based on a technical protocol. This protocol is confidential and shall not be made publicly available.

1.2.2. DigiSign PKI Participants

DigiSign PKI Participants refers to those entities which are filling the role of a participant within DigiSign PKI, either by making use of or by providing the certification services. The participants are identified as follows:

- Certification Authorities
- Registration Authorities
- Validation Authorities
- Subscribers
- Subjects
- Relying Parties
- Other related participants, such as: Repository, TSA Authorities etc.

A. Certification Authorities

A.1. Primary Certification Authorities

DigiSign as a QTSP uses DigiSign Root Certification Authority as a Primary Certification Authority (hereinafter PCA), with the role of point of trust for DigiSign's customers and interested parties. A Primary Certification Authority within DigiSign domain operates based on a self-signed certificate issued by itself. The PCA can issue and sign certificates only to subordinated Certification Authorities.

The PCA certificate does not contain the *certificatePolicies* extension in its structure, which means that there are no limitations for the set of certification paths to which that PCA certificate can be attached to.

A Primary Certification Authority renders certification services to itself (issues and renews its own certificates) and to Intermediate CAs, subordinated to it.

A.2. Intermediate Certification Authorities

Before beginning the activity, every Intermediate Certification Authority must send a request to the Primary Certification Authority, for registration and public key certificate issuance. All intermediate CAs within DigiSign domain are being identified as described below.

Intermediate Certification Authority	Policy Identifier[1]
DigiSign Qualified CA Class 3 2017	1.3.6.1.4.1.34285.1.2.4.256.2.1.3
DigiSign Production Transfond Qualified DS CA	1.3.6.1.4.1.34285.256.10.3.20141030
DigiSign Production Transfond Simple SSL CA	1.3.6.1.4.1.34285.256.10.4.20141030
DigiSign Test Transfond Qualified DS CA	1.3.6.1.4.1.34285.256.10.5.20141030
DigiSign Test Transfond Simple SSL CA	1.3.6.1.4.1.34285.256.10.6.20141030
DIGISIGN TRANSFOND EBUSINESS QUALIFIED DS CA	1.3.6.1.4.1.34285.256.10.3.20141030
DIGISIGN TRANSFOND EBUSINESS SIMPLE SSL CA	1.3.6.1.4.1.34285.256.10.3.20141030
DigiSign for BNR Qualified DS Production CA V2	1.3.6.1.4.1.34285.1.2.4.256.1.1.2.3
DigiSign for BNR Simple SSL Production CA V2	1.3.6.1.4.1.34285.1.2.4.256.1.1.2.3
DigiSign for BNR Qualified DS Test CA V2	1.3.6.1.4.1.34285.1.2.1.256.1.1.2.0
DigiSign for BNR Simple SSL Test CA V2	1.3.6.1.4.1.34285.1.2.1.256.1.1.2.0

Table 1 – Policy Identifiers for Intermediate CAs certificates

B. Registration Authorities

A Registration Authority (hereinafter RA) assists a Certification Authority by performing tasks such as identifying the Subject and authentication of Subject's requests for registration, renewal, suspension or revocation of certificates.

The RA receives, checks, and approves or rejects the registration form, the requests for issuance or renewal of certificates and the revocation/suspension requests. Furthermore, the RA can submit applications to the corresponding CA in order to cancel an applicant request or to withdraw a certificate.

The RA plays a crucial role in the certification process due to its task of verifying the Subject's identity. The level of assurance regarding the Subject's identity relies on the identification process conducted by the RA and it is imposed by the class of the certificate requested by the Subject. In the case of the simplest identification process, a Registration Authority checks only the correctness of the submitted e-mail address. The most precise identification process requires the Subject's attendance in person (physical presence) to one of the Registration Authorities and submission of proofs for his identity. The identification process might be carried either automatically, either manually by one of the RA's Officer.

In order to ensure a high quality of the services it provides, DigiSign relies on a dedicated network of Registration Authorities.

The RAs, in specific, operates tasks such as registration of Subject's, validation of Subject's identity, submission of Subject's requests, forms and documents and delivery of cryptographic devices. The provision of RAs services is compliance with this CPS and is ensured by DigiSign's subcontractors under a signed contractual agreement with DIGISIGN S.A. The list of authorized RAs within DigiSign domain is publicly available at www.digisign.ro.

[1] OID structure [1.3.6.1.4.1.34285]: 1 – ISO; 3 – Identified Organization; 6 – DOD; 1 – Internet; 4 – Private; 1 – Enterprise; 34285 – DigiSIgn's IANA assigned number.

C. Validation Authorities

Validation Authorities within DigiSign domain contain three different services: real time validation through OCSP, validation of issued certificate through CRLs and verification of issued certificate by consulting the electronic register of issued certificates. All these services are described in chapter 4.10 of this document.

D. Subjects

The Subject is the entity whose identifier is placed in the field *Subject* of a certificate and who does not issue a certificate to other entities, in case of the certificates issued for end users.

The Subject of a certificate issued by DigiSign CAs can be:

- a natural person;
- a natural person identified in association with a legal person (the certificate contains attributes regarding the organization linked with the subject);
- a legal person;

Also, the authorities within DigiSign domain can be the Subject of a certificate (e.g. the Certification Authorities which issues certificates or the Time-Stamping Authorities which issues the time-stamps).

E. Subscribers

The Subscriber represents the entity which makes a request to DigiSign, in order to obtain one or more certificates. In most cases, the Subscriber is the Subject itself, but there are cases in which the Subscriber acts on behalf of one or more distinct Subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company). Thus, given the type of certificate requested, a Subscriber can be:
a. when requesting a certificate for natural person:

- the natural person itself,
- a natural person mandated to represent the Subject,
- a legal person with which the natural person is associated.

b. when requesting a certificate for legal person:

- a natural person which is the legal representative of the Subscriber,
- any entity as allowed under the relevant legal system to represent the legal person.

DigiSign issues different types of certificates and of different assurance levels. Subscribers must decide what type of certificate is the most suitable for their needs. In order to be eligible for receiving CA services, the Subscriber shall comply with the requirements related to the appropriate certificate application procedure and to the Subscriber's obligations and liabilities as stated in the CPS.

To avoid any conflicts of interests, the Subscriber and DigiSign as a QTSP shall be separate entities. This rule is subject to an exception: the organization running all or a part of the RA activities within DigiSign domain, can have the quality of a Subscriber when requesting certificates for itself or for persons identified in association with him/her/it.

D. Relying Parties

The Relying Party represents entities such as persons or devices, which relies on a certificate and/or on a cryptographic operation verifiable with reference to a public key listed in the certificate.

A Relying Party[2] uses the Subscriber's certificate either to validate the electronic signature and/or electronic Time-Stamp applied with that certificate, either to interrogate the identity of the source or the author of a message or to create a secret communication channel with the owner of the certificate.

In order to verify a certificate they intend to use in a cryptographic operation, the Relying Parties must always verify the issuer CA's validation service (e.g. OCSP, CRL, Public Electronic Register etc) and the Certificate Policy information, prior to relying on the information featured in that certificate.

By relying on a certificate issued by DigiSign CAs, the Relying Parties declare that they also comply with the Relying Parties obligations and liabilities laid out in this CPS.

A Relying Party is responsible for how it checks the current status of a Subscriber's certificate. A Relying Party must use the information contained by the certificate (for example, identifiers and qualifiers of certification policy) to decide whether a certificate was used according to the stated purpose.

E. Other participants

Amongst the above stated participants, in the certification process some other entities play an important role. Such entities may be represented by the Time-Stamping Authorities and DigiSign's Repository.
The Repository administrated by DigiSign is publicly available at www.digisign.ro and represents a web-based interface to the following information, but not limited to:

- policies, practices and public statements of DigiSign
- information regarding the trust services DigiSign is providing to End Users
- the public electronic register of certificates and time stamps
- the public keys of DigiSign CAs certificates

The Repository is described in detail on the next chapters of this document. The Time-Stamping Authorities are not subject to this CPS. Details on the public statements regarding the Time-Stamping Authorities within DigiSign domain are published in DigiSign's repository.

1.3. Applicability area of the certificates

A digital certificate (or commonly named Certificate) represents formatted data which cryptographically binds an identified entity with a public key. A certificate allows an entity, taking part in an electronic transaction, to prove its identity to other participants in such transaction. Different types of certificates are used in commercial environments as a digital equivalent of an identification card.

A time-stamping token cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time in that particular form.

Certificates issued pursuant to this CPS may be used for several different scenarios (e.g. to sign). However, the sensitivity of the information processed or protected by a certificate varies greatly. Thus, every Relying Party must evaluate the application environment and associated risks before deciding on whether to use a specific type of certificates issued under this CPS.

[2] A Relying Party can be an entity that is not necessary a Subscriber as well. Both the Relying Party and the Subscriber are End Users within DigiSign domain.

1.3.1. Appropriate certificate uses

The certificate usage defines the scope in which a certificate may be used. This scope is defined by two elements: the certificate applicability (e.g. electronic signature, encryption etc) and the allowed or prohibited applications.

This CPS covers certificates which can be used to process and insure the information security with different assurance levels. The assurance level needed must be assessed by the Subscriber and/or Relying Party. s

The following table provides a brief description of the appropriate use, given the level of assurance. The description is for guidance and is not binding.

Nr. Crt.	Level of Assurance	Certification Policy Name	Appropriate Use
1	High	Qualified	This class of certificates provides the highest level of assurance when it comes to the subject's identity. This level corresponds to environments where the chances of data compromising are very high and where consequences of a security incident are very serious. These certificates are usually recommended to protect transactions of unlimited value and transactions with a high level of fraud occurrence. Qualified certificates for electronic signatures can be used for authentication and creation and validation of electronic signatures and time stamps. Qualified certificates for electronic seals can be used for authentication and creation and validation of electronic signatures and time stamps.

The Relying Parties are responsible for setting the information sensitivity level, and thus the necessary level of assurance of a certificate used for a certain purpose. Taking into consideration the significant risk factors, the Relying Parties must decide what type of certificate best meets the formulated requests. Subscribers must know the requirements of the Relying Parties (for example, the electronic signature must be a qualified one) and then request to DigiSign the issuance of a certificate corresponding with those requirements.

1.3.2. Recommended applicability area

DigiSign issues different type of certificate, each according with different applicability areas, as following:

a. CA certificates - their usage is not restricted to a definite area; the applicability area might result from the extension in the certificate that settles how the private key may be used or its role (for example, Subscriber, Certification Authority or other authority that provides PKI services); this type also contains operational certificates of the Certification Authorities;

b. TSA certificates - are issued to servers which, as a response to a Subscriber's request, issue time stamps binding some data (documents, messages, electronic signatures etc.) to a moment of time based on which it can be determined the data sequence in time;

c. VA certificates - they are issued for servers that function in compliance with OCSP protocol and provide information regarding the certificates' status;

d. End-User certificates for:

- **demo/testing**: these certificates are intended for End-User usage and only for demonstration or testing the functionalities in a specific application. Their intended usage can be customized as per request (e.g. authentication, encryption etc).
- **encryption**: these certificates are intended only for encrypting and decrypting electronic data in order to ensure confidentiality and privacy of information.
- **authentication**: these certificates are intended to ensure the authentication of the certificate subject in a particular system.
- **signing/sealing**: these certificates are intended for applying electronic signatures/seals to a document or a message.
- **qualified signatures/seals**: these certificates are intended for applying qualified electronic signatures/seals to documents or messages, providing them legal value.
- **code signing**: these certificates are used by programmers in order to protect their software against forgery.

1.3.3. Prohibited usage

It is prohibited to use digital certificates issued by CAs within DigiSign domain for other purposes than those stated above.

No matter the level of assurance of a certificate, there is no guarantee that the Subject of the certificate is trustworthy, honest or reputable in its business dealings, compliant with any laws or safe to do business with. A certificate only establishes that the information in the certificate was verified in accordance with this CPS when the certificate was issued (e.g. code signing certificates do not indicate that the signed code is safe to install or free from malware, bugs or vulnerabilities).

1.4. CPS Management

This chapter describes the procedures followed by DigiSign in order to develop and maintain both the Certification Practice Statements and Certification Policies within DigiSign domain. This chapter targets the procedures for approving those documents, as well as the nature of changes that lead to the issuance of new policies.

1.4.1. Organization administering the document

The Certification Practice Statements and the Certification Policies within DigiSign domain are administered by DIGISIGN S.A. through its Policies and Procedures Management Body.

Policies and Procedures Management Body is composed of the senior management of DIGISIGN S.A. The procedure used to add or remove members of this body is determined and ruled by internal documents which are not public.

1.4.2. CPS publication and notification

This CPS is available for any interested party in an electronic form on DigiSign's official website: www.digisign.ro. There is no need for special credentials in order to access the document. This CPS can also be provided on request either at office@digisign.ro, either by postal mail at the coordinates mentioned in above.

DigiSign may publish four versions of the CPS, as follows: the currently applicable version, the previous version and the version under approval, if applicable. The status of this CPS shall be highlighted on the first page. All PKI Participants should take into account the version of the CPS that has the status „currently applicable version", that being the version they have to comply with.

The version with the status „under approval" is the new version developed by DigiSign and published for comments for 30 days, if applicable.

This CPS is at its 3rd edition, being written in both English and Romanian language.

2. Publication and repository responsibilities

DigiSign's repository is available for public consultation at www.digisign.ro with no need for credentials for access, and contains the following:

- Policies and Practice Statements and Disclosure Statements of Certification and Time-Stamping Authorities within DigiSign domain;
- Terms and Conditions regarding the provision of trust services by DigiSign
- Certificates of ROOT CAs and Intermediate Cas within DigiSign domain, as well as the appropriate CRLs;
- Certificates of Subjects;
- Other relevant documents, such as DigiSign's certifications and assessments.

The availability of the repository is designed to exceed 99% of business hours, defined as 24 hours out of 24, 7 days a week, excluding planned maintenance periods which are announced first, with 24 hours in advance.

In case of unavailability due to a natural disaster, such as a catastrophe, DigiSign shall make best endeavors to reinstate availability of the service within 24 hours.

DigiSign's ensures the authenticity of the information published in the repository, by implementing logical and physical protection mechanism against unauthorized additions, deletions or modifications. DigiSign may take reasonable measures in order to protect against and prevent from abusive usage of repository, OCSP and CRL download services.

If DigiSign discovers a breach of security (e.g. the integrity of the Repository has been affected), then it shall take appropriate actions to reestablish the integrity and will inform immediately the affected entities. DigiSign may impose legal actions for those who are guilty of the security breach.

DigiSign publishes information on the repository with the following frequency:

Information	Frequency
Policies, practices and disclosure statements	According to Chapter 1.4
Terms and Conditions	After every update
Root and Intermediate Certificates	After every new issuance
Subject's certificates	After every new issuance, when the consent has been obtained

Certification, assessments and audit reports	After DigiSign receives them
Additional information	When necessary

3. Identification and authentication

The chapter hereby describes general rules for checking the Subject's identity, rules that apply when issuing a certificate by DigiSign. These are based on information included in certificates and mention the indispensable means to ensure that the information is precise and credible when issuing the certificate.

The checking is mandatory performed in the stage of Subject's data registration and modification as well as upon DigiSign's request in case of any other certification service.

3.1. Naming

DigiSign issues certificates in compliance with X.509 v3 standard, which means that the certificate issuer and the RA that acts on behalf of the issuer approve the Subject's name in compliance with X.509 v3 standard.

Basic names of the subject and of the certificate issuer, placed in certificates issued by DigiSign, are in compliance with the Distinctive Name (hereinafter DN) – also known as directory names, created following the X.500 series recommendations, IETF RFC 5280 and ETSI standards.

Subject and certificate issuer DNs are meaningful in Romanian language, as well as in any other Latin language. The structure of the DN, approved, designated and checked by DigiSign RA, depends on the subject's type.

The name of the Subject must be confirmed by an operator of the Registration Authority and approved by a Certification Authority. DigiSign ensures (within its domain) the uniqueness of the DNs.

Over the life time of a CA within DigiSign domain, a distinguished name which has been used in a certificate by it, shall never be re-assigned to another entity.

For natural persons, DN consists of the following fields, mandatory or not:

Field	Meaning
C	International abbreviation for country name (RO for Romania), conform to ISO 3166-1 alpha-2
S	County / District where the Subject lives
L	Residence city of the Subject
CN	Subject's name
O	Name of the institution where the subject works
OU	Name of the department where the subject is hired
T	Name of subject's function
SN	Subject's surname
G	Subject's first name / given name
P / Pseudonym	Subject's nickname used in his environment or which wants to use not to disclose his real first name or surname
SN	Personal identification code of the subject

For legal persons, DN consists of the following fields, mandatory or not:

Field	Meaning
C	International abbreviation for country name (RO for Romania), conform to ISO 3166-1 alpha-2
O	Name of the organization
OU	Name of the organization's department
S	County / District where the organization functions
L	Residence city of the organization
CN	Name of the organization
organizationIdentifier	Legal person semantics identifier

The option of using a pseudonym is allowed to the applicants provided that they don't use expressions that are established as inappropriate or which involve fraudulent usurpation of a known name/person or that implies a parody of a person.

3.2. Initial identity validation

DigiSign verifies the identity of the Subject prior to the issuance of the certificate. The identity validation process differs depending on the certificate type and usage and it is described as follows. After the identity validation process is successfully concluded, DigiSign checks that the certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

In order for DigiSign to be able to verify the Subject's identity, the Subject shall provide DigiSign with evidence regarding his/hers/its supposed identity. The submitted evidence may be in form of either paper or electronic documentation, but in both cases the RA shall validate their authenticity.

If the Subscriber does not coincide with the Subject of the certificate (e.g. the company that requiring certificates for its employees to allow them to participate in electronic business on behalf of the company), then the Subscriber shall provide contact data and evidence that he/she/it is authorized to act on behalf of the Subject, at least:

- Full name of the Subscriber,
- A proof of the agreement of representation, if the Subscriber represents a natural person,
- When the Subscriber represents a legal person (either for requesting a certificate for that legal person or to request a certificate for a natural person identified in association with the legal person), an agreement that the subscriber is allowed to represent the legal person and is entitled to request certificates for that legal person,
- If the Subscriber is not a natural person, it shall be represented by a natural person whose authorization to represent the Subscriber shall be proved.

Every Subject that requests services specific to public key infrastructures and requests the issuing of a certificate shall (prior to the certificate issuance):

- Fill in an on-line registration form or a document that may be downloaded from DigiSign's Web site,
- Submit evidence regarding the Subject's identity,
- Generate a RSA asymmetric key pair (software or on a qualified secure cryptographic device, for qualified certificates) and provide the Registration Authority the prove of owning a private key; alternatively, the Subscriber may delegate a Certification Authority or the Registration Authority to generate this key pair,

- Suggest a distinctive name
- If applicable, fill in and send a registration form that contains a public key and the prove of owning its corresponding private key,
- Optionally, attend the Registration Authority and provide the required documents (if required by the certification policy based on which the certificate is issued),
- Conclude an agreement with DigiSign; the present CPS is part of this agreement,
- if applicable, provide documents attesting to professional qualifications and the right to sign for adding specific attributes to the certificate.

Depending on the level of assurance of each certificate, the Subject shall provide more or less evidence, as follows. According to this CPS, DigiSign issues qualified electronic certificates with a high level of assurance, describing below the conditions under which this type of certificate is being issued.

A. Certificates with no level of assurance

The issuance of certificates with no level of assurance implies a thin identity validation. In this case, the RA verifies only the domain which hosts the e-mail address provided by the Subject in the registration form. No other validation is conducted by the RA prior to the issuance of this type of certificate.

B. Certificates with a low level of assurance

For certificates with a low level of assurance, the Subjects shall provide evidence regarding their supposed identity, depending on the Subject's type:

a. If the Subject is a natural person, evidence shall be provided of at least:
   - Full name,
   - Date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

b. If the Subject is a natural person who is identified in association with a legal person, evidence shall be provided of at least:
   - Full name of the Subject,
   - Date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which can be used to, as far as possible, distinguish the person from others with the same name,
   - Full name and legal status of the associated legal person,
   - Any relevant existing registration information of the associated legal person,
   - Affiliation of the natural person to the legal person and approval by the legal person that the Subject's attributes identify that legal person (e.g. a procuration from the legal person).

c. If the Subject is a legal person, evidence shall be provided of at least:
   - Full name of the legal person
   - When applicable, the association between the legal person and the organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate.

The issuance of certificates with a low level of assurance implies a process of identity validation which regards the following:

- The RA collects evidence of the Subject's supposed identity (e.g. a copy of an identification document) and if applicable, evidence of any specific attributes of the Subject;
- The RA confronts the data collected from the registration form with the evidence submitted;

- If the data corresponds with the submitted evidence, the RA approves the certification application and sends a request to the CA to issue the certificate;
- If the data does not correspond with the submitted evidence, the RA rejects the certification application and informs the applicant about it.

C. Certificates with a substantial level of assurance

For certificates with a substantial level of assurance, the Subjects shall provide the same evidence regarding their supposed identity as per certificates with a low level of assurance. In case of certificates with a substantial level of assurance, the Subject must submit the evidence of their supposed identity in person or by a duly mandated Subscriber which represents the Subject. In the latter, the Subject shall be identified by a public authorized Romanian notary.

The issuance of certificates with a substantial level of assurance implies a process of identity validation which regards the following:

- The RA collects evidence of the Subject's supposed identity (e.g. the original form of an identification document) and if applicable, evidence of any specific attributes of the Subject;
- The RA confronts the data collected from the registration form with the evidence submitted;
- The evidence of the Subject's identity shall be checked by the RA against the natural person either directly by physical presence of the person (the Subject shall be witnessed in person unless a duly mandated Subscriber represents the Subject, case in which the duly mandated Subscriber must be as well witnessed in person) or shall have been checked indirectly using means which provides equivalent assurance of the physical presence (e.g. the Subject is identified by a public Romanian authorized notary);
- If the data corresponds with the submitted evidence, the RA approves the certification application and sends a request to the CA to issue the certificate;
- If the data does not correspond with the submitted evidence, the RA rejects the certification application and informs the applicant about it.

D. Certificates with a high level of assurance

For certificates with a high level of assurance, the conditions presented above applies.

Furthermore, for this type of certificates, the following additions applies:

a. For qualified certificates issued to natural persons, the identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:
    - by the physical presence of the natural person at the authorized RA within DigiSign domain; or
    - by the physical presence of the natural person at a public Romanian authorized notary; or
    - using methods which provide equivalent assurance in terms of reliability to the physical presence and for which DigiSign proves the equivalence, such as identification and authentication of the Subject using a valid qualified electronic certificate issued by DigiSign; or
    - Using remote identification methods, with video support that allow the verification of security elements for the presented identity documents and offer the DigiSign operator the possibility to verify and validate the concordance between the natural person and documents; or
    - by a third party, abiding by the national legislation in force in the field of identity certification/confirmation.

Using remote identification methods, with video support, the natural person, if he opts for video identification, will enter into a secure video identification performing the process in an automated manner following the instructions displayed on screen. During the video identification session, the user presents the identity document for verification, validates the code sent via SMS, smiles at the camera. The video identification is verified by the DigiSign operator and validates and verifies the data of identity, deciding whether the identity validation is accepted or not.

b. For qualified certificates issued to legal persons, the identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:
   - by the physical presence of an authorized representative of the legal person, at the authorized RA within DigiSign domain; or
   - by the physical presence of an authorized representative of the legal person, at a public Romanian authorized notary; or
   - using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which DigiSign proved the equivalence, such as identification and authentication of the Subject using a valid qualified electronic certificate issued by DigiSign; or
   - Using methods that provide an equivalent level of assurance from the perspective of reliability with physical presence; or
   - by a third party, abiding by the national legislation in force in the field of identity certification/confirmation.

For qualified electronic certificates, the private key shall always be generated using a QSCD. An entity may have a QSCD when generating the key or the entity may delegate DigiSign to generate the private key on its behalf. In this latter case, DigiSign guarantees that the QSCD and the key is securely sent to that entity, in accordance with Chapter 6.1. - Key pair generation and installation.

DigiSign identifies and defines clear objectives regarding the quality and security of the remote identification process of individuals, in particular regarding resilience to cases of false acceptance and false rejection of applicants.
These indicators apply to all cases provided for in the identification process described in this document, including in situations involving physical presence, according to the requirements defined in the applicable standard.
The objectives aim to:

- Minimize the probability of accepting an inauthentic person;
- Minimize the probability of rejecting an authentic person;
- Maintain the balance between the two risks to ensure a secure and fair process.

The provider regularly conducts internal performance tests to assess the extent to which the established objectives are achieved and, where appropriate, adjusts the procedures, technical means or training of the personnel involved.

3.3. Identification and authentication for rekey and renewal requests

The procedure for certificates rekey and renewal are described in Chapter 4.7. – Certificate renewal and rekey.

All requests regarding certificate renewal or rekey have to be concluded by filling in the appropriate registration form. The requests are processed by the RA which shall ensure that the requests are complete, accurate and authorized.

All requirements laid out in Chapter 3.2. – Initial identity validation regarding the evidence and the procedure which has to be followed in order to prove identity, applies also for the rekey and renewal requests. In particular, some additional requirements have to be met, as follows:

- The RA within DigiSign domain shall check the existence and validity of the certificate, in case of renewal: the initial certificate has to be valid (not revoked, not suspended) and there has to be at least 5 days until expiration.
- The RA shall ensure that the Subject has read the Terms and Conditions and that the Subject has agreed with those provisions, even if the Terms and Conditions hasn't been changed meanwhile.

In case of modification of the initial data, the Subject has to submit evidence regarding the new information or the updated once, in accordance with the procedures laid out in Chapter 3.2. – Initial identity validation.

3.4. Identification and authentication for revocation or suspension requests

Revocation and/or suspension requests can be sent either online, via e-mail at suport@digisign.ro, either offline in printed form through the Registration Authorities or directly to DigiSign's headquarters.

The revocation and/or suspension requests are sent by filling in a form which aims data like information about the certificate's Subject and the reason for which the request is made (e.g. the private key was lost or stolen). All requests are being processed on receipt. The form may aim more than one certificate and has to be signed by the certificate's Subject.

Upon receiving the signed form, the Subject's identity is being verified (consistency of submitted data with data declared through other means). Only if the RA has successfully concluded the identity validation procedure, a request is sent to the CA with details about the certificate that has to be revoked/suspended.

All requests regarding the revocation or suspension of a certificate are, prior to any action being taken, authenticated by checking if they came from an authorized source.

4. Certificate life cycle operational requirements

This chapter describes the procedures regarding the registration, identification and authentication of the subject and the issuance of certificates.

DigiSign has made available for any interested party all information related to the electronic trust services it provides based on electronic certificates. Although not the subject of this document, DigiSign has also published all information regarding additional products and services it provides, like certificates for web authentication, electronic time stamps, secure cryptographic devices and secure creation and validation of signatures application.

DigiSign publishes all this information in a comprehensible manner, making them available in an electronically (downloadable) format at www.digisign.ro, as well as upon request in printed form, in order for any interested party to make an informed decision prior to the submission of an application. Moreover, DigiSign has made available 24 hours out of 24, 7 days out of 7, the Support Department which can assist any interested party with understanding the information regarding DigiSign's provision of services.

Moreover, at the Customer Service Office, the interested party has the opportunity for survey and consultation. The Customer Service Office is available at DigiSign's headquarters from Monday to Friday, from 9 AM till 5 PM.

4.1. Registration form

Prior to the certificate application, a registration request must be submitted by the applicant to DigiSign. In order to ease the Subscriber registration process and to reduce the amount of errors, an End User web based registration preparation interface is provided to any interested party. This interface presents to the Subscriber with a convenient and intelligent electronic form, which has the role to collect information needed for registration. This form shall dynamically present appropriate fields, depending on the choices made by the Subscriber: type of requested certificate, type of identity etc.

Through this registration form, an applicant shall specify the type of certificate they request and their data, which will be indicated in the certificate. Also, by completing the registration form, the applicant shall authorize DigiSign for the management of their personal data, in order for DigiSign to successfully full fil its obligations as a QTSP.

The registration form shall at least contain the following:

- data to be indicated in the certificate
- personal identification information of the Subject
- personal identification information of the person entitled to represent the Subject (e.g. in case of certificates issued for legal persons)
- billing and delivery information

After the registration form is completed, the applicant shall receive via e-mail a set of documents containing the terms and conditions for the provision of the service, such as parties' obligations, liabilities, rights and other related information.

DigiSign processes all information collected through the registration form, in accordance with the applicable data protection legislation. In this regard, DigiSign processes the personal data of the applicant in accordance with the requirements of Regulation (EU) No. 910/2014 and in compliance with the internal provisions of Regulation No. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and other provisions of Union common law on data protection.

4.2. Certification application

DigiSign does not take into consideration the data indicated in the registration form, unless the applicant confirms it by submitting the certificate application.

The certificate application consists of signed documents needed for the certificate issuance or renewal, and the validation of Subject's identity by the Registration Authority, according to the certificate's level of assurance. Details about the documents and the Subject's identification are presented in Chapter 3 – Identification and authentication.

The certificate application can also include a public key. If so, the key must be prepared so that it could cryptographically connect the public key with other data specified in the request, especially with the Subject's identification data. A request may contain instead of the public key, the Subject's request to generate an asymmetric key on his name. This might be fulfilled by a Certification Authority or by the

Registration Authority. Following the generation, the keys are sent on secured path to the Subject so that they cannot be activated by an unauthorized person.

Unless otherwise specified by law, a certificate application can be submitted by anyone who complies with the provisions laid out in DigiSign CP and CPS, as well as with the provisions set within the registration forms and the Subscriber's agreement.

Certificate application may only be submitted by natural persons, which can request a certificate either for themselves or for the legal person they represent.

Certificate application can be submitted by the applicant to the Registration Authority's operators or to the appropriate Certification Authority. In case the applicant sends the certificate application to the RA, the RA operator verifies it and decides either to approve it and send the request of issuance to the CA, either to reject it and send it back to the applicant for corrections (if the case).

An authorized third party can submit a certificate application instead of the applicant only if he/she presents a document, authenticated by a public notary, which states that he/she is entitled by the Subject or the Subject's legal representative to submit the certification application to DigiSign.

4.3. Enrollment process

DigSign accepts requests individually submitted and only on electronic form. The requests sent online are submitted via WWW pages, using secure HTTP (HTTPS) protocol on DigiSign's servers at www.digisign.ro. An applicant that wants to send a request, visits DigiSign's website and fills in the registration form, in compliance with the instructions on site. The form can be filled in by a Registration Authority operator at the Subscriber's demand.

Before being officially entitled and operational, DigiSign RA's operators are trained and are subject to regular audit done by DigiSign in order to ensure a highly trusted operational environment.

The certification application can be, on the other hand, submitted online, offline or using certified video identification. The certification application submitted online are applicable only in the case of certificate's renewal.

The certification application sent offline may be done as follows:

- by the applicant physical personal attendance or the physical attendance of the organization's representative or hardware device/software code owner, at the Registration Authority or at the Certification Authority.
- through an authorized third party, complying with the requirements set out in the present document regarding the identification and authentication of the subject.
- through physical mail, complying with the requirements set out in the present document regarding the identification and authentication of the subject.

Every certification application is processed by the RA as follows:

- RA's operator receives the Subscriber's application
- The operator verifies the data from the application and identifies the Subject
- The operator verifies the proof of the private key possession, in accordance with Chapter 3.2 - Initial identity validation
- The RA operator verifies also other data that are not specified in the application, but which are necessary for issuing the certificate

- Following the verification, the RA operator confirms the identity between the data stated and the data included in the application; if the application contains non-compliant data it is rejected
- The confirmed application is then sent as a request by the RA to the appropriate Certification Authority within DigiSign domain.

Every request sent to a Certification Authority is, prior to the issuance of a certificate, checked by the CA if it was confirmed (approved) by the RA.

4.4. Certificate issuance

The request received from the RA are being examined by the CA within a period of maximum 5 (five) working days by the CA. This period depends mainly on the accuracy of the data sent by the Subscriber and the cooperation between DigiSign and the applicant. In case the missing or incorrect data is not made available to the CA in time, or there are additional documents needed, the issuance term will be extended accordingly.

After receiving and processing a request confirmed by the RA, the CA issues the certificate following a specific procedure:

- The processed request is sent to the certificate issuance server
- If the application contains the request to generate a key pair on behalf of the Subscriber, the server asks the hardware key generator to do so
- The quality of the public key generated is being tested
- If the actions are successfully concluded, the server issues a certificate and delegates the hardware security module to sign the certificate
- The certificate is stored in the CA's database
- The CA prepares a response containing the issued certificate and sends it to the Subscriber
- If the actions weren't successfully concluded, then the CA rejects the request

DigiSign can refuse the issuance of a certificate to any solicitor without taking any obligations or responsibility for the possible losses or damages affecting the Subscriber as following to the rejection. In this case, DigiSign will refund the solicitor the certificate fee (if the fee was paid prior to the issuance request), excepting the case when the solicitor provided false data to DigiSign. The certificate issuance rejection may occur in the following situations:

- if there are suspicions or certainties concerning the forgery or usage of false data by the Subscriber,
- if the Subscriber, in an inconvenient manner, engages resources and processing means of DigiSign, by submitting a number of requests clearly in excess of his needs,
- other reasons besides those stated above.

Information concerning the decision made by the CA and its reasons are sent to the solicitor. The solicitor may request again the issuance of a certificate, but only after the reasons that lead to the rejection are solved.

DigiSign informs the Subscriber about the issuance of the certificate by electronic mail. This method consists of sending (at the e-mail address rendered by the Subscriber) a notification regarding the issuance of the certificate and, in case of submitting the certification application online, together with the notification is being sent also the public key certificate.

4.5. Certificate acceptance and publication

When receiving a certificate, the Subscriber is committed to check its content, especially the data correctness and the complementariness of the public key with the private key owned. If the certificate has any faults or mistakes that cannot be accepted, the Subscriber is obliged to immediately inform the CA and to request the certificate revocation.

The certificate is considered accepted by the Subject after the first use or after the period of time defined in the Terms and Conditions (e.g. five days after receiving it), whichever event occurs first. The certificate is considered received when the Subscriber receives the package sent by DigiSign which contains the certificate. In the case in which the Subscribers sends online the certificate application, the certificate is being considered received by the Subscribed at the date when the notification about the issuance is being sent.

In case the certificate is being rejected, the Subscriber and/or Subject has the obligation to return the QSCD which stores that certificate to DigiSign and to request its revocation.

If the certificate is not rejected and the DigiSign is not being notified within the period of time set out in the Terms and Conditions, the certificate is considered accepted. The certificate is also considered accepted once the Subscriber makes use of it no matther what cryptographic operation is made with that certificate and regardless of the number of days that had passed since the certificate has been received.

If the Subscriber submitted the certification application at DigiSign headquarters, the acceptance of the certificate is considered explicit and coincides with the moment when the certificate Subject sign a proof that he/she received the certificate.

Every accepted certificate is published by DigiSign in the Electronic Public Register of Certificates and is available for the public at www.digisign.ro. Once published in the EPR, it is considered that every interested party (e.g. Relying Parties) was notified about the issuance of the certificate.

4.6. Certificate applicability and key usage

The Subscribers must use the private keys and the certificates as follows:

- in compliance with the purposes laid out in the present CPS and in compliance with the certificate's content
- in compliance with the provisions of the agreement between DigiSign and the Subscriber
- only during the certificate's validity period

The Relying Parties must use the public keys and certificates as follows:

- in compliance with the provisions set out in the CP and CPS
- only after the proper verification of the certificate and the issuer's certificate

4.7. Certificate rekey

DigiSign offers the following types of rekey: certificate renewal and rekey. The difference between the two lays in the fact that the certificate renewal can only be requested if the initial certificate is valid (not revoked, not suspended), has at least 5 days until expiration and the request does not imply the modification of essential data (e.g. subject's name or e-mail address).

4.7.1. Rekey

Rekey is done when a Subscriber, which already has an electronic certificate, generates a new key pair or orders to the CA to generate the key pair, and requests the issuance of a new certificate.

The rekey is done when the Subscriber's initial certificate has expired or has less than 5 days until expiration and when essential data has been changed. Also, the procedure applies for altered certificates or in the case of malfunction of the device that contains that certificate.

The rekey procedure implies the same steps as the issuance of a certificate described in prior chapters and, unlike the certificate renewal, the modification of Subject's data is allowed. The rekey procedure also implies the validation of Subject's identity as described in Chapter 2 – Identification and authentication. The provision regarding the registration forms, the certification application, the enrollment process and certificate acceptance applies to the rekey procedure.

DigiSign always informs the Subscribers (with at least 45 days before) about the approach of the certificate's expiration.

4.7.2. Certificate renewal

The certificate renewal represents the replacement of the certificate in use (currently valid) with a new certificate which contains the same data regarding the Subject, but a new validity period and a new unique serial number. This procedure also refers to the possibility of a certificate modification, but only regarding to that data which are not considered essential, such as optional fields within the certificate (e.g. the Title).

In order for a Subscriber to be able to apply for a certificate renewal, a set of conditions have to be met:

- The initial certificate has to be valid (not revoked, not suspended) and with at least 5 (five) days until expiration
- The Subscriber hasn't changed his/hers/its personal data (e.g. the identification document used in order to issue the certificate in the first place)
- The Subscriber performs a request for certificate renewal in compliance with the instructions published at www.digisign.ro.

In order for a certificate to be renewed, the Subscribers has to submit a request to DigiSign by filling in a form through the intelligent form application at www.digisign.ro. The authentication of the request its made through the Subject's qualified electronic certificate. If the Subject doesn't have anymore access to its initial certificate and the key pair, he/she/it must undertake the rekey procedure as described in the previous chapter.

The requests for certificate renewal must be processed and confirmed by the Registration Authority.

4.8. Certificate revocation

A certificate status can be valid, suspended or revoked. While a suspension is a temporary and reversible state, the revocation process is irreversible. Once revoked, the certificate can not be un-revoked, but a certificate can be un-suspended (reactivated) to become valid again.

All requests regarding the revocation of a certificate shall be submitted to DigiSign as soon as possible since the moment any of the circumstances stated in section 4.8.2 happened.

4.8.1. Who can request a revocation

The following entities can send certificate revocation requests:

- The Subject itself;
- The Subscriber, if applicable; in this case, the Subject is duly informed about the request;
- An authorized representative of the Certification Authority (such as the Security Administrator);
- A Subject's mandatory, only with an authorized and authenticated procuration issued by a public authorized notary;
- The RA on behalf of the Subject
- The RA for its own, only[3] if it has substantial information that justifies the certificate revocation
- The authority or organization that issued the documents attesting to professional qualifications and the right to sign, in the case of certificates that include specific attributes.

The RA can submit the revocation request only if there are substantial information that justify the request (e.g. the RA has information regarding the private key being compromised) or if the certificate has been suspended for more than a period of 30 days.

4.8.2. Circumstances for revocation

A revocation request must be submitted if:

- The private key is lost, stolen or potentially compromised[4],
- The Subject no longer has sole control of the private key because the private key activation data (e.g. the PIN code) has been compromised or for any other reason,
- The certified data is not reflecting the certificate request as verified by the Subject in the acceptance period, in accordance with the provision laid out in this CPS,
- The certified data has become inaccurate or has changed in any way (e.g. if the Subject has changed his/hers/its name),
- The parties (DigiSign and the Subscriber and/or Subject) decide to terminate the contract concluded between them,
- The certificate has been suspended for more than a period of 30 days,
- In any other case in which the Subscriber and/or Subject does not comply with this CPS, the Certification Policy or the agreement concluded with DigiSign,
- The holder of the digital certificate no longer holds the professional capacity and right to sign, in the case of certificates that include specific attributes.

Certificates belonging to a Certification Authority within DigiSign domain can be revoked by the issuing CA. Such a revocation may appear in the following situations:

- The CA has reasons to believe that the data within the respective certificate do not correspond to the reality,
- The private key of the CA or its informatic system were compromised, case in which all certificates issued by this CA must be revoked along with the CA's certificate,
- The CA terminates its activity, case in which all certificates issued by this CA must be revoked along with the CA's certificate,
- The CA violated the material obligations of the present CPS, the Certification Policy or the agreement.

[3] The Registration Authorities within DigiSign domain acts with extreme caution when processing revocation requests that were not sent by the Subject and accepts only those requests in compliance with this CPS.

[4] The private key compromised means: (1) unauthorized access to the private key or a strong reason that determine to believe such thing, (2) private key loss or occurrence of a reason to suspect such a loss, (3) private key stolen or occurrence of a reason to suspect such a robbery, (4) accidental deleting of the private key.

4.8.3. Procedure for revocation

DigiSign made available for all interested parties, a procedure regarding the steps which have to be made by a solicitor in order for a certificate to be revoked. This procedure is available online at DigiSign's official website, or by request via e-mail at suport@digisign.ro Also, the procedure can be obtained in printed form at DigiSign's RA.

The procedure implies the submission of a form which contains data about the requestor, the certificate that needs to be revoked and the reason of the request.

The form shall be submitted to DigiSign, signed either with a handwritten signature, either with the qualified electronic signature of the requestor, as follows:

- by e-mail, at suport@digisign.ro,
- by physical mail submitted to RAs within DigiSign's domain.

All revocation requests are processed on receipt, after they are previously authenticated and confirmed by the RA, as follows:

1. If the form is being submitted through a RA within DigiSign domain:
   - the requestor is being identified by the RA operator, in order to establish if the requestor is authorized or not to make such a request;
   - the RA confirms with the requestor, by phone, the data contained in the form, such as the certificate information and reason for revocation. If the form is being submitted through the RA at DigiSign's headquarters, then RA confirm the data contained by the form in the same time with the identification of the requestor;
   - if the data is being confirmed, the RA sends a request for revocation to the CA;
   - the CA authenticate if the request came from an authorized RA (if not, rejects the request);
   - the CA revokes the certificate and changes the status from active to revoked.

2. If the form is being submitted by e-mail:
   - the requestor is being identified through the qualified electronic signature applied on the form. If the form is handwritten signed, than the requestor is identified by confirming a code he/she is in possession of;
   - the RA confirms with the requestor, by phone, the data contained in the form, such as the certificate information and reason for revocation and, if applicable, the requestor code for identity confirmation;
   - if the data is being confirmed, the RA sends a request for revocation to the CA;
   - the CA authenticate if the request came from an authorized RA (if not, rejects the request);
   - the CA revokes the certificate and changes the status from active to revoked.

The revocation of a certificate is definitive. DigiSign always notifies the Subject and if applicable, the Subscriber, with regards of the certificate revocation, irrespective of who made the request or the reason of revocation.

DigiSign makes its best effort to ensure that the time needed to process the revocation request and to publish the revocation notification (updating the CRL) shall be reduced as possible and does not exceed 24 hours.

4.9. Certificate suspension

While the revocation of the certificate is definitive, the suspension is a reversible process. All requests regarding the suspension of a certificate shall be submitted to DigiSign as soon as possible since the moment any of the circumstances stated in section 4.9.2 happened.

4.9.1. Who can request a suspension

The persons or entities who can request the suspension of a certificate are limited to the persons or entities who can request the revocation of a certificate, as specified under section 4.8.1.

4.9.2. Circumstances for suspension

A suspension request shall be submitted if:

- the revocation request cannot be processed due to RA being out of working hours,
- the information within the certificate no longer correspond to reality, if the revocation of the certificate is not required,
- an injunction disposes the suspension,
- if the Subscriber/Subject delays or does not pay the appropriate fees due to the issuance of the certificate,
- in any other situation that needs further explanations from the Subscriber/Subject,
- the holder of the digital certificate no longer holds the professional capacity and right to sign, in the case of certificates that include specific attributes.

4.9.3. Procedure for suspension

The procedure for certificate's suspension is the same as the revocation procedure. After successfully verifying the request, the CA changes the state of the certificate into *certificateHold*.

DigiSign always notifies the Subject and if applicable, the Subscriber, with regards of the certificate suspension, irrespective of who made the request or the reason of suspension.

A certificate cannot be suspended for more than 30 days. If more than 30 days have passed, then the certificate will be revoked. DigiSign shall notify the Subject and if applicable, the Subscriber, about this action.

4.9.4. Un-suspension of a certificate

If the reasons for which a certificate is suspended, has ceased, then the CA can cancel the suspension. The persons whom may request the un-suspension and the procedure are the same as for the suspension of a certificate, described in Chapter 4.9. – Certificate suspension.

After the un-suspension (reactivation) is successfully concluded, the certificate is eliminated from the Certificate Revocation List, but the period in which it was suspended will remain registered in the Public Electronic Register.

4.10. Certificate status and verification

Upon revocation, suspension or un-suspension, the certificate's status changes and this information is stored in DigiSign's database. Every change in the certificate status is traceable through (1) the Certificate Revocation List (CRL), in compliance with the publishing periods of the CRLs, (2) the OCSP services and (3) the Public Electronic Certificate.

The maximum delay between the confirmation of the revocation/suspension/un-suspension to become effective and the actual change of the status information of that certificate being made available to interested parties is at most 60 minutes. Usually, regarding the OCSP services and PEC, this happens immediately.

4.10.1. CRL verification

Every Certification Authority within DigiSign domain issues a CRL. A new CRL for intermediate Certification Authorities is published in every 24 hours, with the validity period of 48 hours, the time being synchronized with UTC. The CRLs for the ROOT CAs within DigiSign domain are issued at least yearly under the condition that there are no certificate revocations meanwhile. In case of ROOT CA certificate revocation, that certificate is immediately published in the CRL.

The CRL profiles are described in this document under Chapter 7.2. – CRL Profiles.

A Relying Party as following of receiving a document electronically signed by the Subscriber, is committed to verify if the public key certificate corresponding to the private key of the Subscriber used for creating electronic signature is not placed in the Certificate Revocation List. The Relying Party is committed to use the current and updated CRL.

A certificate's status verification may be based exclusively on CRL only in case the CRL's issuing period frequency stated by DigiSign cannot bring any important damage or loss for the Relying Party. Otherwise, a Relying Party is committed to contact (by phone, fax etc.) the certificate issuing authority or to use the *on-line* certificate status verification service provided by the DigiSign Validation Authority (VA).

If a certificate to be checked is placed in a CRL, the Relying Party is committed to reject the document associated to this certificate if the revocation reason is one of the following:

a. *unspecified* – not known
b. *keyCompromise* – compromise of the private key security
c. *cACompriomise* – compromise of the Certification Authority security
d. *cessationOFOperation* – termination of the services associated to the private key
e. *certificateHold* – certificate suspension

If a certificate was revoked for one of the following reasons:

f. *affiliationChanged* – data modification
g. *superseded* – key modification

The final decision over the certificate's credibility will be taken by the Relying Party. When taking this decision the Relying Party must take into consideration that the reason specified in paragraph above, lit f, g, which do not represent the Subscriber's private key compromise.

4.10.2. OCSP verification

DigiSign provides the online certificate status verification service in real time. This service is realized based on the OCSP protocol described in RFC 6960. Using OCSP it is possible to obtain more exact data (compared to the exclusive usage of the CRL) concerning a certificate status.
OCSP functions on the basis of the request-response model. As response to a request the OCSP server provides the following information about the certificate status:

- *good* – meaning a positive response to a request that must be seen as confirmation for the certificate validity,

- *revoked* – meaning the certificate was revoked,
- *unknown* – meaning the certificate was not issued by one of DigiSign CAs.

The OCSP service is available online, for any interested party that wants to verify a certificate issued with DigiSign CAs.

Certificate status is always provided in real time (at the moment of the request) based on information from DigiSign's VA database and contains information newer that those from the published CRLs.

4.10.3. Public Electronic Register

All certificates issued by DigiSign are published in the Public Electronic Register (PEC). If the status of the certificate changes, the status published in PEC also changes.

Furthermore, if a certificate has been suspended for a period of time and un-suspended subsequently, the period of time in which the certificate has been suspended shall be registered in PEC for future verification of signed documents with that certificate.

The PEC makes also available the certificate in different formats (e.g. DER or PEM).

5. Facility, management and operational controls

DigiSign, as a provider of qualified trust services for the issuance, renewal, suspension, revocation, validation and generally successful administration of issued digital certificates, puts security at the heart of its activities. In order for all its assets, activities and services to be secure, DigiSign has implemented, maintains and continuously improves an information security management system certified SR EN ISO/IEC 27001:2023. In accordance with the requirements of this security framework, all security activities begin with a risk assessment to identify and classify all information assets, to assess the risks to which they are exposed and to determine the necessary technical, managerial, organizational and procedural controls. DigiSign maintains an inventory of all information assets and assigns them a classification consistent with the risk assessment. All those controls related to CA and RA assets and activities comply with the applicable requirements of the following standards:

- ETSI EN 319 401, General requirements regarding the policies of Trust Service Providers,
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for Trust Service Providers issuing EU qualified certificates;

Further, this chapter shall describe general requirements regarding physical, organizational and personnel security controls. For safety reasons, DigiSign will not describe the specific measures taken in security controls. The documents describing the implementation of security controls within DigiSign are considered confidential.

5.1. Physical security controls

Physical security controls implemented by DigiSign are designed to protect both software (the logic layer) and hardware (physical layer) of DigiSign PKI against unauthorized use. Computer systems, operator terminals and information resources within DigiSign are disposed in a dedicated area, physically protected against unauthorized access, destruction or disruption of activity. These areas are permanently monitored and each entry and exit is recorded in an event log. Furthermore, the stability of electricity supply and temperature are continuously monitored and controlled.

5.1.1. Site location

DigiSign headquarters is located in 74B Nicolae G. Caranfil street, 014146, 1st District, Bucharest, Romania.

DigiSign facility and Certification Authority are publicly available every working day between 9 AM and 5 PM. In the remaining time, including non-working days and holidays, the facility is available only to persons authorized by DigiSign management.

5.1.2. Physical access

Trust services provided by DigiSign relies on secured premises regarding the hosting of DigiSign CAs. DigiSign is using physically separated space in server rooms, specifically designed for data center operations. The equipment of DigiSign CAs is permanently protected from unauthorized access. DigiSign RA physical access controls are also implemented to minimize any risk. These security mechanisms are appropriate to the threat level in the space where the RA's equipment is installed.

DigiSign systems are protected by five levels of physical security as follows:

a. Level 1 access – requires an identification document (Identification Card, Passport etc) which is presented to the guard at reception. Access to this level is both automatically monitored (video system) and manually registered (through a register book where the guard is writing data about every person that comes and gets out of the building).
b. Level 2 access – requires a proximity card access, limited to the corresponding floor which when used is automatically monitored and recorded.
c. Level 3 access – requires individual access control for all persons entering the RA and CA area through the use of the biometric fingerprint system. This level of access is automatically monitored.
d. Level 4 access – refers to access inside the cage located in the datacenter. Physical access is prohibited at this level for all visitors and employees with lower level of access. This level of access is automatically monitored.
e. Level 5 access – refers to the biometric access to the racks located inside the cage and requires individual access control. The key ceremony room requires dual control, each using two factor authentication: biometric fingerprint system and proximity card. This level of access is automatically monitored.

5.1.3. Power and air conditioning

DigiSign facility is equipped with heating, ventilation and air conditioning systems to control the temperature and relative humidity, in order to offer an adequate operating environment. Also, there are power systems to ensure uninterrupted access to electric power. If a power cut occurs, the emergency power source (UPS) ensures undisturbed continuation of the activity until the automatic intervention of the building power back-up generator.

5.1.4. Water exposure

DigiSign has taken reasonable precautions to minimize the impact of water exposure to the information systems. The risk of flood in the server area is minimal due to its position: about 1 meter distance above the ground.

5.1.5. Fire prevention

DigiSign has taken reasonable precautions to prevent and extinguish fires or others damaging exposure to flame or smoke. DigiSign facility benefits of a fire prevention and extinction system in compliance with the corresponding standards and regulations in this field.

5.1.6. Media storage

In accordance with the requirements of the Information Classification, Labeling and Management Procedure, media containing data or backup information are stored in a highly secure area. Access to this area is allowed only to authorized persons. All storage areas are protected against fire and water exposure and damage.

5.1.5. Waste disposal

Waste disposal is securely implemented in order to prevent unauthorized disclosure of sensitive data. Paper and electronic media containing information significant for DigiSign's security are destroyed after expiration of the retention period. Hardware security modules are reset and deleted in compliance with the manufacturer's recommendations. These devices are, as well, reset and deleted when sent to service or repaired.

5.1.6. Off-site backup

Backup media are securely stored in a separated location from the original media location and are protected against fire and water exposure. DigiSign has implemented measures to ensure full recovery of its services in case of a disaster, corrupted server, software or data, within 48 hours. Backup and disaster recovery sites are located in separate premises sufficiently distant from the primary location and benefit from equivalent security measures.

5.2. Procedural controls

The operational security controls implemented by DigiSign for both CA and TSA activities ensures that CA/TSA systems are secure and correctly operated with minimal risk of failure.

This chapter describes a list of roles which can be defined for personnel employed in DigiSign and also the responsibilities and duties associated with each defined role.

5.2.1. Trusted roles

DigiSign ensures that personnel have achieved trusted status and departmental InfoSec approval is given before such personnel is entrusted with access devices and electronic credentials to access and perform specific functions on DigiSign's systems.

The following trusted roles which shall be manned with one or more individuals are applied within DigiSign:

a. Security Officers: are responsible for implementing security policies and procedures.
b. Certificate system administrators: they are responsible for the installation, configuration, maintenance and upkeep of the certification system.
c. Network administrators: are responsible for the installation, configuration and maintenance of network equipment.

d. System Auditor: is authorized to access archives and audit logs of CA's trusted systems. Is responsible for conducting internal audits for compliance with the CPP by the CA; This responsibility also extends to RAs operating within DigiSign.
e. Suspension and revocation operators: they are responsible for suspension and revocation of the certificates.
f. RA operators: on behalf of the RA, they are responsible for carrying out the duties outlined in conformity with DigiSign procedures specified for the identification and registration of subscribers.

Within DigiSign, the auditor role cannot be combined with any other role. No entity that has a different role than the auditor can take over the auditor's responsibilities.
Employees are formally assigned trusted roles by the DigiSign Policy Management Body. The principle of "least privilege" is applied when configuring access privileges to trusted roles

5.2.2. Number of people required to perform a sensitive task

DigiSign has established, maintains and enforces rigorous control procedures in order to ensure the segregation of duties based on job responsibilities, as well to ensure that multiple trusted persons are required to perform sensitive tasks.

The following activities require a minimum of two different types of trusted persons: key generation, key backup, key restauration, management of HSMs and CAs core systems, physical visits to data centers.

Key generation process (for certificate and CRL signing) is one of the main operations which requires particular attention. This activity requires the presence of at least two trusted persons or, it can also be observed by shared secret holders who retain their part of the key in a secure location.

5.2.3. Identification and authentication for each role

DigiSign has implemented an access control system which identifies and registers all users in a trustworthy manner.

DigiSign personnel are subject to identification and authentication procedures, as follows:
a. placement on the list of persons allowed to access DigiSign facilities
b. placement on the list of persons allowed to physically access system and network resources of DigiSign
c. issuance of confirmation authorizing to perform the assigned role
d. assignation of credentials (account and password) in DigiSign's information system

Every assigned account has to be unique and directly assigned to a specific person, it cannot be shared with any other person and has to be restricted according to the function arising from the role performed by a specific person on DigiSign's software system.

Operations performed in DigiSign's systems, that require access through shared network resources, are protected with implemented mechanisms of strong authentication and encryption of transmitted information.

5.3. Personnel controls

Personnel security controls are documented in policies which are not public and include topics covered by the next sub-sections.

5.3.1. Qualifications, experience and clearance requirements

DigiSign ensures that the persons performing his/hers responsibilities, arising from the acted role in DigiSign PKI, has:

a. graduated from at least the high school
b. signed an agreement describing his/hers role in the system and the corresponding responsibilities
c. been subject to advanced training on the range of obligations and tasks associated with his/her position
d. been trained in the field of personal data protection and confidential and private information protection
e. signed an agreement containing clause concerning sensitive information protection and confidentiality and privacy of subject's data
f. been informed that he/her shall not perform tasks which may lead to a conflict of interests between a CA or RA acting on behalf of it.

Managerial personnel possess expertise and training in PKI technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

DigiSign ensures that all members of the personnel staff that are involved in the provision of trust services, are checked regarding qualifications, expert knowledge, experience and clearance needed and as appropriate to fill trusted roles and to perform the related specific job function. Such checks are specifically directed towards misrepresentations by the candidate, appropriateness of validated references and any clearance of deemed appropriate.

5.3.2. Background check procedures

DigiSign makes or ensures that the relevant checks are performed to prospective personnel by means of status reports issued by competent authority, third party statements or self statements.

5.3.4. Training requirements and retraining frequency

DigiSign's employees have received training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

Personnel performing roles and tasks arising form the employment in DigiSign or its LRAs have to complete training as to regard to:

a. regulations of CPP and CP
b. procedures and security controls employed by CAs and RAs
c. system software of CAs and RAs
d. responsibilities arising from roles and tasks performed in the system
e. procedures executed upon system malfunction or corruption to a CA/RA

Upon completion of the training, all participants shall sign a document confirming their familiarization with the CPSs and CPs, as well as acceptance of associated restrictions and obligations.

DigiSign ensures that all personnel performing managerial duties, received comprehensive awareness training regarding the security principles and rules within DigiSign, the internal regulations and processes, as well as the duties they are expected to perform.

The training is carried out periodically (at least annually) and whenever there are significant changes in the operation mode of DigiSign or RA.

5.3.3. Job rotation sequence and frequency

Not applicable.

5.3.4. Unauthorized actions and sanctions

In case of a discovery or suspicion of unauthorized access, DigiSign management may suspend the perpetrator's access to DigiSign systems, if the perpetrator is a DigiSign employee. Disciplinary actions for such accidents shall be described in suitable regulations and should comply with the applicable law.

5.3.5. Independent contractor requirements

Independent contract personnel (external service, developers of subsystems or applications, etc.) are subjected to the same verification procedure as employees of DigiSign. Additionally, contract personnel, when performing their task at DigiSign facility have to be escorted by DigiSign employees, except those who have previous approval from the security administrator.

5.3.6. Documentation supplied to personnel

DigiSign makes the relevant documentation or ensures that the relevant documentation are provided to members of DigiSign personnel staff, in order for them to carry out their specific job functions. Documentation distribution shall occur during initial training, retraining and whenever otherwise appropriate.

DigiSign shall provide to its personnel with access to the following documents:

a. CPP and CP
b. range of responsibilities and obligations associated with the acted role in the system
c. Policy and security procedures.

5.4. Audit logging procedures

5.4.1. Type of events recorded

Every DigiSign security-critical activity is recorded in event logs and archived. Archives are stored on storage media that cannot be easily overwritten or destroyed (unless transferred to long-term storage media) for the period of time they are required to be kept. DigiSign event logs contain records of all activities generated by the software components within the system.
The type of data recorded by DigiSign include but are not limited to:

- all events relating to registration including requests for certificate, rekey or renewal, maintaining the privacy of subject information, such as:
  - documents presented by the applicant to support registration
  - record of unique identification documents
  - storage location of copies of applications and identification documents (e.g. signed subscriber agreement)

  - any specific choices in the subscriber agreement (e.g. consent to publication of certificate)
  - the identity of the entity accepting the application
  - method used to validate identification documents, if applicable
  - name of the submitting RA, if applicable.
- all events regarding the life-cycle of CA keys and certificates issued
- all events relating to the life cycle of keys managed by a CA within DigiSign domain, including any subject keys generated by a CA
- all requests and reports relating to revocation, as well as the resulting action.

Security events such as security profile changes, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts, are also logged.

5.4.2. Frequency of processing logs

The audit trail is audited when an abnormal event occurs (whenever necessary).

5.4.3. Retention period for audit logs

The logs are kept until the expiration of the last certificate issued by a CA within DigiSign domain.

5.4.4. Protection of audit logs

The logs can be accessed only by people authorized by DigiSign Management. Each modification of logs is made only with authorization.

5.4.5. Audit log backup procedures

Audit logs are backed-up regularly on DR site.

5.4.6. Vulnerability assessments

To properly secure DigiSign's information technology assets, the information security & risk team assess the security stance periodically by conducting regular vulnerability assessments at least twice a year and penetration test at least once a year. With the outcomes of these activities DIGISIGN can apply security fixes or other compensating controls to improve the security of the environments.

The techniques used during the security assessments aim to cover a range of methodologies and attack techniques as broad as possible in order to identify all the plausible cyber risks. For this reason are used automated scanning tools as well as manual techniques.

5.5. Records archival

Logs regarding the certificate lifecycle are retained as archive records for a period no less than 10 (ten) years, especially for the qualified certificates.

Regardless of their storage media, archives are protected in integrity, and are only accessible by authorized personnel. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period required.

Records concerning the operation of services are made available to legal authorities and/or persons whose right of access to them arises from the law.

5.6. Compromise and Disaster Recovery

In the event of a disaster, including compromise of the private signing key or trust service credentials and failure of critical components of DigiSign's trustworthy systems, operations shall be restored as soon as possible. In this matter, DigiSign has defined and is maintaining a CA Compromise procedure and Business Continuity Plan to enact in case of a disaster.

DigiSign CA Compromise procedure and Business Continuity Plan includes solutions for the system data backup and recovery, CA key compromise, revocation status and algorithm compromise.

5.6.1. Incident and compromise handling procedures

DigiSign has implemented a business continuity plan, which covers procedures of risk assessment, incident handling (includes a response to incidents and disasters), recovery and recovery exercises.

DigiSign carries out an annual risk assessment of DigiSign's Trust Services to prevent possible danger to the availability of DigiSign's operations and to minimize the risk of losing control of the Trust Services. The list of situations considered as emergency situations is determined by the risk assessment. The result of the risk assessment includes the requirements for recovery plans and recovery testing scenarios.

The recovery plans and testing scenarios include at least the following threats:

- for DigiSign CA and DigiSign TSA, the private key used for the provisioning of the service is compromised or there is a serious suspicion thereof;
- for DigiSign TSA, the loss of synchronisation of a time-stamping service clock.

The procedures for the handling of information security incidents, emergency situations and critical vulnerabilities are documented in the internal DigiSign's Incident Reporting and Management Procedure. The objective of that regulation is the immediate response and recovery of availability and the continuous protection of DigiSign services.

In the event of an emergency, DigiSign will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency situation and proposed solution through public information communication channels.

DigiSign will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body in Romania (The Authority for the Digitalization of Romania) and, where applicable, other relevant bodies as national DNSC or The National Supervisory Authority For Personal Data Processing of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

5.6.2. Computing Resources, Software, and/or Data are Corrupted

The event of the corruption of computer resources, software and data is handled according to DigiSign's internal Security Incident Management Policy.

5.6.3. CA private key compromise

The compromise of a key of the CA will lead to the immediate revocation of all issued certificates. In such a case, the various participants will be notified that the CRL may not necessarily be fully trusted, in accordance with the procedure for liability to a compromised CA.

5.6.3. Algorithm compromise

In case of algorithms or associated parameters, used by DigiSign or its subscribers, become insufficient for their remaining intended usage, DigiSign shall inform all subscribers and relying parties of the algorithm being compromised and schedule a revocation of any affected certificate after the announcement.

5.7. CA or RA termination

The provision of the trust services shall be terminated:

a. with a decision of DigiSign's Executive Management Committee
b. with a justifiable decision of the authority exercising supervision: the Romanian Supervisory Body - The Authority for the Digitalization of Romania
c. with a final and irrevocable judicial decision
d. upon the liquidation or termination of the operations of DigiSign.

Before DigiSign terminates the provision of a trust service, the following procedures shall be executed:

- DigiSign informs the following about the termination: all subscribers and relying parties, as well as all entities with which DigiSign has agreements or other forms of established relations
- DigiSign makes the best effort for doing arrangements with other Trust Service Provider to transfer the provision of services for its existing customers
- DigiSign destroys the CA and TSA private keys, including the backup copies or the keys withdrawn form use in such manner that the private keys cannot be retrieved
- DigiSign reinitializes and/or destroys any hardware appliances related to the services being terminated, depending on the security regulations in force
- DigiSign terminates all authorization of all subcontractors to act on behalf of DigiSign in carrying out any functions relating to the process of issuing trust services

The notification regarding DigiSign's CAs termination shall be published in the public media.

DigiSign does not assume liability for any loss or damage as a result of CA termination, provided that DigiSign has given public notice of termination throughout public communication channels at least one month in advance.

DigiSign has taken out a liability insurance policy to cover the costs to fulfill the above minimum requirements in case DigiSign goes bankrupt or for any other reasons is unable to cover the costs by itself.

These requirements are applicable also in case of Delegated Registration Authorities termination.

6. Technical security controls

This chapter describes procedures used for the generation and management of the cryptographic key pair of a CA and a Subscriber, as well as associated technical requirements.

6.1. Key pair generation and installation

DigiSign uses cryptographic keys generated and installed in a safety manner and follows industry best practices for key lifecycle management, key length and algorithms.

All keys must be generated using a FIPS or Common Criteria-approved methods.

6.1.1. Key pair generation

Key pair generation is a critic process given that the way how the key pair is generated is essential to the safety of the entire PKI system.

a. Root CAs Keys

DigiSign Root CAs key pairs are created in accordance with the internal procedures for creating this type of keys. DigiSign's Root CA Key Pairs are generated by multiple trusted individuals, acting in trusted roles and using a secure cryptographic hardware device (HSM), FIPS 140-2 Level 3 certified, as part of a scripted key generation ceremony. The HSM activation requires the use of a two-factor authentication tokens. The HSM protects the keys from external compromise and operates in a physically secure environment.

DigiSign follows a documented procedure (key ceremony) for conducting the Root CAs key pair generation regarding all its Root CAs. DigiSign produces a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. The procedure and the report are not publicly available.

Each DigiSign Root CA owns one self-signed certificate. The private key corresponding to the public key contained in the self-signed certificate is used exclusively to sign the public keys of the intermediate CAs by signing the operational certificates and the CRL necessary for the authorities functioning. A similar purpose is intended for the private keys held by each intermediate CA, corresponding to the public keys included in certificates issued by the Root CAs for each authority.

Upon key pair generation for certificate and CRL signing, private key distribution and its activation in hardware security module, the keys can be used in cryptographic operations until the validity period has expired or the keys have been revealed.

DigiSign ROOT CAs cryptographic keys have a limited lifetime period; if the period has expired, the keys shall be updated.

b. (Intermediate) CAs Keys

The keys of intermediate CAs are generated within DigiSign facility, in the presence of a trusted group of persons. The key pairs are generated on designated, authenticated workstations that are connected to a HSM, FIPS 140-2 Level 3 certified. The key pairs are permanently retained encrypted on the HSM.

The actions executed while performing key pair generation are recorded, dated an signed by each person present during the generation. The records are retained for the needs of audits and common system reviews.

c. Subscribers (end-user) Keys

For qualified electronic certificates issued on QSCD, the key pair shall always be generated and stored into the QSCD.

The Subscriber has the option to generate its own pair of keys. In this case, the key pair has to be verified by DigiSign in order to ensure that it was generated and stored in a secure cryptographic device (QSCD), that meets or exceeds FIPS 140-2 Level 2, 3 or Common Criteria EAL 4, 5 certification standards. When key generation is done by the subject, the certificate request process ensures that the subject has possession of the private key associated with the public key presented for certification, and that the procedure of issuing the certificate is securely linked to the associated registration or certificate renewal.

Likewise, the Subscriber can entrust DigiSign to generate and store the key pair using appropriate applications and secure cryptographic devices (QSCDs), FIPS 140-2 Level 2, 3 or Common Criteria EAL 4, 5 certified. In this case, DigiSign has to securely send the device to the subject.

DigiSign guarantees that in any moment after generation of a key pair on subject's demand, the keys will not be used for creating an electronic signature and that the Certification Authority will not create conditions for making the signature available to any unauthorized entity, except for the owner of the private key.

For unqualified electronic certificates, used in demonstration or for testing purposes, the Subscriber has the possibility to either generate and store the key pair on a secure cryptographic device or in PKCS#12 containers.

6.1.2. Private key delivery to subscriber

If the subject entrust DigiSign with the key pair generation, the keys are thus distributed to the subject as follows:

a. the keys are stored in a secure cryptographic device or in PKCS#12 containers, being delivered to the subject personally or by means of registered mail;
b. the information needed to access the key pair (PIN code) are delivered to the subject either personally or by means of registered mail.

6.1.3. Subject's public key delivery to the CA

Subscribers submit their generated public keys as an electronic request whose format has to comply with protocols of PKCS#10 (CRS).

Requests submitted to a Certification Authority may, in particular cases, require confirmation issued by the Registration Authority.

Submission of a public key is expendable in the case when a key pair is generated on Subscriber's demand or on Registration Authority operator's demand by a Certification Authority, which simultaneously issues a certificate for the generated key pair.

6.1.4. CA public key delivery to Relying Parties

Public keys of CAs issuing certificates to subjects (end-users) are distributed solely in a certificate form, complying with ITU-T X.509 v.3 recommendations. In the case of DigiSign ROOT CAs, certificates are self-signed.

DigiSign CAs public keys are securely provided to potential Relying Parties using the following channels:

a. placement in the publicly available repository of DigiSign; retrieval of the certificates requires the Subscribers to visit DigiSign's official website,
b. distribution of DigiSign's Trust Chain.

6.1.5. Key size

DigiSign follows NIST Special Publication 800-133 (2012) – Recommendation for Cryptographic Key Generation, for recommended timelines and best practices regarding the key size for Root CAs, Intermediate CAs, as well as for End-Users Certificates. Thus, the key pairs must have a sufficient length in order to prevent the private key deduction, using properly cryptanalysis processes.

DigiSign selects from the following key sizes/hash algorithms for Root Certificates, Issuing CA Certificates and End-Users Certificates, as well as for CRL/OCSP Certificate status responder:

- 2048 bit RSA key with secure hash algorithm 2 (SHA-2)
- 4096 bit RSA key with secure hash algorithm 2 (SHA-2)

6.1.6. Public key generation parameters

The creator of a key is responsible for checking the parameter quality of the generated key. He/she is required to verify:

a. ability to execute encryption and decryption operation, including electronic signature creation and its verification,
b. key generation process, which should be based on strong random cryptographic number generators – physical sources of white noise, if possible,
c. immunity to known attacks (applies to RSA and DSA algorithms).

6.1.7. Key usage

Allowed key usage purposes are described in KeyUsage field of standard extension of a certificate complying with X.509 v3. Usage of bits of KeyUsage field has to comply with the following:

a. digitalSignature: certificate intended for creation and verification of electronic signature;
b. nonRepudiation: certificate intended to provide a non-repudiation service by private individuals, as well as for other purposes than described in f) and g). NonRepudiation bit may be set only in a public key certificate intended to verify electronic signatures and should not be combined with purposes described in points c)-e) and connected with providing confidentiality;
c. keyEncipherment: intended to encrypt symmetric algorithm keys, providing data confidentiality;
d. dataEncipherment: intended to encryption of Subscriber's data, other than described in c) and e);
e. keyAgreement: intended for protocols of key exchange;
f. keyDigiSign: public key is used for electronic signature verification in certificates issued by entities providing certification services;
g. cRLSign: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by the entities providing certification services;
h. encipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data encryption in key exchange protocols;

i. decipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data decryption in key exchange protocols.

6.2. Private key protection and cryptographic module engineering controls

DigiSign generate and stores the private key employing a secure system preventing private key loss, revelation, modification or unauthorized access. If a CA generates a key pair on authorized Subject's demand, it has to deliver it securely to the Subject and enforce the protection of the private key.

6.2.1. Standards for cryptographic modules

For the issuance of qualified certificates, DigiSign uses a secure hardware module (HSM) which complies with FIPS 140-2 Level 3 standard. The physical access to this device is restricted by a secure access control system and it can't be activated unless there are at least two authorized persons simultaneously.

Regarding the cryptographic devices used by DigiSign to issue qualified certificates with the private key residing in a QSCD, on authorized subject's demand, DigiSign uses secure cryptographic devices (QSCDs) which complies with FIPS 140-2 Level 2, 3 or Common Criteria EAL 4, 5 standards.

6.2.2. Private key control (N out of M)

DigiSign's services uses hardware modules which requires the participation of more than one person in order to fulfill sensitive tasks. All the necessary tools for the achievement of such operations are safely stored and can't be accessed without the information held by multiple trusted persons. Multi-person control of a private key applies to private keys of CAs certificates.

The multi access control is realized by delivering secrets to authorized and trusted operators. The secrets are stored on cryptographic cards or tokens, protected by a PIN code and transferred authenticated to their owner.

6.2.3. Private key escrow

Key escrow is not allowed for CAs key pairs or Subscribers key pairs.

DigiSign may provide escrow services for other types of key pairs (e.g. key pairs used only for encryption/decryption), in order to provide key recovery. In this case, the escrowed private key is encrypted and protected using the same or a higher level of security as used to generate and deliver the private key.

6.2.4. Private key backup

Certification Authorities operating within DigiSign create a backup copy of their private keys. When the keys are transferred to other media for backup and disaster recovery purposes in an encrypted form. The copies are used in the case of execution of standard or emergency (e.g. after disaster) key recovery procedure. The CAs key pairs are backed up by multiple trusted individuals, using a secure cryptographic hardware device, as part of a scripted and recorded key backup process.

6.2.5. Private key archival

DigiSign does not archive private keys.

6.2.6. Private key transfer into or from a cryptographic module

All keys are generated by and in a cryptographic module. Private keys are exported from the cryptographic module into FIPS 140-2 certified secure backup tokens only for HSM transfer, offline storage or secure backup purposes. The private keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiSign encrypts the private keys and protects the keys used for encryption from disclosure. Private keys used to encrypt backups are securely stored and requires multi person access.

6.2.7. Private key storage on cryptographic module

DigiSign's CAs private keys are generated and stored inside a secure cryptographic module which has been evaluated to at least FIPS 140-2 Level 3. ROOT Private Keys are stored offline in cryptographic modules, in a safe and secure environment which implies multi person access.

6.2.8. Method of activating private keys

DigiSign's CAs private keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Regarding the Subscribers, they are solely responsible for protecting their private keys. DigiSign recommends using a strong password or equivalent authentication method to prevent unauthorized access or use of private keys. The Subscriber should never reveal, under no exceptions, their private key data activation (e.g. PIN code, password etc).

6.2.9. Method of deactivating private keys

The private keys used by DigiSign's CAs are deactivated through logout procedures on the applicable HSM device, when are not in use. The ROOT private keys are further deactivated by removing them entirely from the storage partition on the HSM device. DigiSign never, under no circumstances, leaves the HSM devices in an active unlocked or unattended state.

DigiSign recommends to its Subscribers to deactivate their private keys when not in use by logout and removal procedures.

6.2.10. Method of destroying private keys

DigiSign authorized personnel, acting in trusted roles, destroys in a secure manner all private keys when no longer needed. Destroying a pair of keys may imply deleting it from all known storage partitions. DigiSign also zeroizes the HSM device and associated backup modules, according to the specifications of the device manufacturer. This action reinitializes the device and overwrites the data with binary zeros. If the zeroization or reinitialization procedure fails, DigiSign shall crush, shred and/or incinerate the device in a manner that destroys the ability to extract any key stored on that device.

DigiSign recommends to its Subscribers to destroy, in a secure manner, their private keys when the corresponding certificate is revoked or expired or if the private key is no longer needed.

6.3. Other aspects of key pair management

Technologically, it is possible to manage the same key pair for both signature creation and data encryption. Notwithstanding that this possibility exists, through this CPS DigiSign does not recommend this practice. Under this CPS, it is prohibited for the CA signing keys used for signing End-Users Certificates and the appropriate CRLs, to be used for any other purposes.

Therefore, this chapter will describe other aspects of key pair management, such as public key archival practices and the validity period of private and public keys used and recommended by DigiSign.

6.3.1. Public key archival

The purpose of public key archival is to create the possibility of verifying electronic signatures after the certificate used for signing had been removed from the Repository. This action is crucial regarding the provision of non-repudiation services, such as time-stamping services or certificate status verification services.

Each CA within DigiSign domain, used for the issuance of End-Users Certificates, archives the public key of the Subscriber to whom a certificate was issued. The Subscriber may also archive locally his/hers certificate, especially when this is a mandatory action, required in order to use the certificate in a specific application.

Public key archives are being protected in a manner preventing unauthorized addition, insertion, modification or erasure. The protection is enforced with authentication of the archiving entity and authorization of their requests.

6.3.2. Certificate operational periods and key pair usage periods

Under this CPS, DigiSign uses appropriately all CA private signing keys and not beyond the end of their life cycle, in accordance with the following table.

Keys owner	Maximum usage period
ROOT Certificates	40 years
Intermediate Certificates	25 years
End-User Certificates	3 years

Table 6.3.2. Maximum usage period of key pairs

6.3.3. Certificates validity

The validity period for end user certificates issued by Certification Authorities DigiSign is up to 3 years from the moment they are issued, without exceeding the validity period of the issuing authority.

In the case of qualified digital certificates that include specific attributes regarding professional quality and signature rights, the validity of the issued certificates will be up to 3 years, but without exceeding the validity of the documents attesting professional quality and signature rights.

6.4. Activation data

Activation data refers to a mean of access to a specific private key. The activation data can be a password, a PIN code, an username and associated password, a shared secret etc, or a combination of these.

Registration Authorities and Certification Authorities operators, as well as other persons performing trusted roles, shall operate passwords immune for brute force attacks when they access sytems which

requires authentication with a pair of keys. DigiSign recommends for its users to also use such strong passwords in their systems.

When accessing a private key, DigiSign recommends the use of a multi-factor authentication procedure, such as a cryptographic device and a authentication phrase (e.g. password).

Shared secrets used for CA private key protection are generated in accordance with the provisions of this CPS and are retained inside dedicated cryptographic cards. The cards are also protected by a PIN code, created in accordance with the requirements of FIPS 140-2s. Shared secrets become activation data after their own activation in the system.

Activation data protection includes activation data control methods preventing from their revelation and depend on the fact whether they are authentication phrases and whether control is enforced on the basis of private key or its activation data distribution into shared secrets. In the case of authentication phrases, the recommendations described in FIPS 112 should be enforced, while protection of shared secrets requires implementation of FIPS 120 standard.

It is recommended that activation data used for private key activation should be protected by means of cryptographic controls and physical access controls. Activation data should not be written down. Though, if it is, the level of their protection should be the same as data protected by the usage of a cryptographic card. Several unsuccessful attempts to access the cryptographic module should result in its blockage and thus, loses of private key. Stored activation data should never be retained together with the cryptographic card.

6.5. Computer security controls

DigiSign ensures that computer security controls are implemented in compliance with the technical standards ETSI EN 319 411-1 and ETSI EN 319 411-2, when these standards imposes higher requirements on certification practices, as well as with ISO 27001:2023 standard.

DigiSign performs security configuration checks, as defined in internal policies, at intervals of up to 12 months.

Tasks of Registration Authorities and Certification Authorities operating within DigiSign are carried out by means of trusted hardware and software.

The servers and computers within DigiSign run on trusted systems, configured and tested using field's best practices. The systems are scanned to detect malicious programs, being protected against spyware, malware and viruses. DigiSign limits the access to production servers to only those who are authorized for such access. General application users do not have accounts on production servers.

DigiSign production network is equipped with firewall solutions in order to protect it against intrusion attempts from inside and outside, as well as to limit the network processes which could cause vulnerabilities in production systems. DigiSign imposes to its operators to use passwords that contain a minimum number of characters and a combination of alphanumeric and special characters, as well as to change them regularly.

Detailed descriptions of implemented computer security controls are available as internal documents.

6.6. Life cycle technical controls

DigiSign ensures that periodic development control, security management and life cycle security controls are implemented in compliance with the technical standards ETSI EN 319 411-1 and ETSI EN 319 411-2, when these standards imposes higher requirements on certification practices, as well as with ISO 27001:2023 standard.

System implementation within DigiSign is compliant with current standards regarding system development and the management of change. Every application, prior to be used for production within DigiSign, is tested in a specific environment for testing. This process is performed by IT staff together with DigiSign's operators from different departments. Testing is made according to predefined test scenarios. Testing data is not to be used in production environment and data from production environment is not to be used in testing processes unless prior it has been depersonalized.

Similar rules apply to hardware components replacement, such as:

a. hardware is supplied in a manner allowing its tracing and evaluation of the route of the component to the place of its installation;
b. replacement hardware delivery is carried out in a manner similar to delivery of original hardware; the replacement is carried out by trusted and trained personnel.

The purpose of security management control is to supervise DigiSign system's functionality providing assurance that the system operates correctly and in accordance with the accepted and implemented configuration. Current configuration of DigiSign system, as well as any modifications and updates to its system are recorded and controlled. Controls applied to DigiSign system allow continuous verification of application integrity, their version and authentication and verification of hardware origin.

Detailed descriptions of implemented computer security controls are available as internal documents.

6.7. Network security controls

DigiSign ensures that network security controls (including but not limited to firewalls, network intrusion detection, secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with ETSI EN 319 411-1 and ETSI EN 319 411-2 standards, when such standards impose higher requirements on certification practices.

Servers and trusted workstations of DigiSign system are connected by a local network (LAN), devised in more sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall. Security controls are developed on the basis of firewall and traffic filtering on the routers and Proxy services.

Means of protection of the network security accept only messages submitted with the usage of HTTP(S), LDAP(S), NTP, POP3(S), IMAP(S) and SMTP(S) protocols. Events (logs) are recorded in the system journals and allow supervision of correctness of the usage of services provided by DigiSign.

Detailed descriptions of implemented computer security controls are available as internal documents.

7. Certificate, CRL and OCSP profiles

This chapter describes certificate, CRL and OCSP profiles employed within DigiSign PKI.

Certificate profiles and Certificate Revocation List profile (CRL) comply with the format described in ITU-T X.509 v.3 standard, while the profile of Online Certificate Status Protocol service (OCSP) complies with the requirements of RFC 6960.

The certificates issued by DigiSign CAs are compliant with the specifications included in ETSI EN 319 412 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1, 2, 3 and 5.

7.1. Certificate profiles

Following the X.509 v.3 standard, a certificate is the sequence of the following fields: the body of certificate (tbsCertificate), information about algorithm used for certificate signing (signatureAlgorithm), and an electronic signature of the Certification Authority (signatureValue).

7.1.1. Certificate content

The contents of a certificate include values of basic fields and extensions (standard, described by norms, and private, defined by the issuing authority). Extensions defined in a certificate according to norms allow assignation of additional attributes to the subject and his/her/its public key and simplify management of hierarchical certificate structure. Certificates issued in accordance with X.509 v.3 standard allow definition of proprietary extensions, unique for a given implementation.

a. Basic fields

DigiSign supports the following basic fields:

- **Version**: third version (X.509 v.3) of certificate format
- **Serial Number**: certificate serial number, unique within Certification Authority domain
- **Signature Algorithm**: identifier of the algorithm applied by a issuing Certification Authority
- **Issuer**: distinguished name (DN) of a Certification Authority,
- **Validity**: validity period, described by the beginning date (notBefore) and the ending date (notAfter) of the certificate,
- **Subject**: distinguished name (DN) of the Subscriber that is the subject of the certificate,
- **Subject Public Key Info**: value of a public key along with the identifier of the used cryptographic algorithm associated with the key.

b. Extensions

Function of every extension is defined by the standard value of the corresponding object identifier. Extension, depending of the choice of issuing authority, may be critical or non-critical. If an extension is defined as critical, the application supporting certificate usage must reject every certificate containing an unrecognized critical extension. On the other hand, extensions defined as non-critical may be omitted.

DigSign supports the following fields of standard extensions:

- **AuthorityKeyIdentifier**: identifier of a Certification Authority public key certificate associated with a private key, used for signing issued certificates – non-critical

- **SubjectKeyIdentifier** – subject key identifier – non-critical

- **KeyUsage**: describes the usage of the key - critical
  digitalsignature (0): key for electronic signature creation
  nonRepudiation (1): key associated with the non-repudiation services
  keyEncipherment (2): key for key exchange
  dataEncipherment (3): key for data encryption
  keyAgreement (4): key for key agreement
  keycertsign (5): key for certificate signing
  CRLsign (6): key for CRL signing
  encipherOnly (7): key only for encryption
  decipherOnly (8): key only for decryption

- **ExtKeyUsage**: defines the constraints related to the key usage – non-critical. This field defines one or more areas, in addition to standard key usage, defined by keyUsage field, of the possible usage of a certificate. This field should be interpreted as constraint of allowed key usage purpose defined in field keyUsage. DigiSign issues certificates which may contain one of the following value or combination of such values in ExtKeyUsage field:
  serverAuth – authentication of TLS Web servers;
  clientAuth – authentication of TLS Web clients;
  codesigning – signature of executable codes;
  emailProtection – E-mail protection;
  ipsecEndSystem – IPSEC protocol protection,
  ipsecTunnel – IPSEC protocol Tunnelling,
  ipsecUser – IP protocol protection in user application,
  timeStamping – binding of the digest value with the time provided by previously accepted trusted time source;
  OCSPsigning – assigns the right to issue certificate status confirmations on behalf of CA;
  dvcs – issuance of confirmation by a notary authority, on the basis of DVCS protocol;
  EncryptedFileSystem – allows the usage of the certificate to encrypt the file system (EFS); it is a mandatory request from certain applications (i.e. EFS);
  SmartCardLogon **–** allows the usage of the certificate for „smart-card logon" operation – authentication in the operating system, based on the digital certificate;

- **Certificate Policies** – the extension indicates the policy (policies) followed by a Certification Authority when issuing certificates – non-critical. The extension is a PolicyInformation list information (identifier, electronic address) about an applied certification policy.

c. Qualifiers

Certificates issued by DigiSign CAs may also include qualifiers, recommended by RFC 3280:

- **PolicyMapping**: this field contains one or more pairs of OID, defining equivalency of the certificate issuer policy with the certificate subject policy – non-critical

- **SubjectAlternativeName:** alternative name of the subject – non-critical

- **BasicConstraints**: defines the certificate type (CA or end entity certificate), as well as the maximum accepted length for the certificate chain – critical

- **CRL DistributionPoints**: the extension defines network addresses hosting the current CRL of the issuer Authority of the respective certificate – non-critical

- **AuthorityInfoAccessSyntax**: the field indicates the method of information and service provision by the issuer of the certificate – non-critical

- **OCSPNoCheck**: if it is included in an OCSP responder certificate, the clients who receive OCSP responses signed with a private key associated to the certificate may trust the certificate status during its availability period; this extension is non-critical and it is defined by the RFC 6960 standard.

- **NetscapeCertType**: this extension limits the certificate usage only to certain applications defined by the extension's value. If it is not present, the certificate may be used for any application except the ObjectSigning applications. This extension is non-critical, and its value may be one of the following combinations:
  SSLClient (bit 0): certificate may be used to authenticate a SSL client
  SSLServer (bit 1): certificate may be used to authenticate a SSL server
  S/MIME (bit 2): certificate may be used by clients of S/MIME secured mail
  ObjectSigning (bit 3): certificate may be used to sign objects such as Java applets or plug-ins
  SSL CA (bit 5): certificate may be used to issue certificates used for SSL
  S/MIME CA (bit 6): certificate may be used to issue certificates used for S/MIME
  ObjectSigning CA (bit 7): certificate may be used for issuing certificates used for ObjectSigning

d. Electronic signature algorithm identifier

The field of signatureAlgorithm contains a cryptographic algorithm identifier used for electronic signature created by a Certification Authority on the certificate. In the case of DigiSign, RSA algorithm is used in combination with SHA-1 and SHA-2 functions.

e. Electronic signature field

The value of the field signatureValue is a result of execution of cryptographic hash function algorithm for all fields of a certificate (tbscertificate) and signing algorithm of the obtained digest with a private key of the authority.

7.1.2. Profiles

A. ROOT CA

DigiSign ROOT Certification Authority	
Version	V3
Serial Number	16 5e 1c 37 56 d0 2b 77
Signature Algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO

Valid From	Thursday, October 30, 2014 12:40:13
Valid To	Monday, October 30, 2034 12:40:13
Subject	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Public Key	
Public Key parameters	05 00
Subject Key Identifier	49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Authority Key Identifier	KeyID=49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Basic Constraints	Subject Type=CA Path Length Constraint=None
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbrint algorithm	sha1
Thumbrint	f5 e3 24 04 2f f4 5e 1c b9 3a a5 a4 46 8c 59 f2 0f 53 dc 5e

B. INTERMEDIATE CA

DigiSign Qualified CA Class 3 2017	
Version	V3
Serial Number	21 00 9b 29 28 2c 68 a6
Signature Algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Valid From	luni, 10 aprilie 2017 13:03:44
Valid To	miercuri, 6 aprilie 2033 13:03:44
Subject	CN = DigiSign Qualified CA Class 3 2017 2.5.4.97 = VATRO-17544945 OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Public Key	
Public Key parameters	05 00
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.34285.256.3.0.2.0.2017 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:

	https://www.digisign.ro/cps
Subject Key Identifier	53 21 f4 13 a6 75 37 49 66 de b3 02 69 9d b0 dc ff 07 19 c7
Authority Key Identifier	KeyID=49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Subject Alternative Name	office@digisign.ro
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.digisign.ro/repository/rootcav3.crl
Authority Information Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.5.46.1) Alternative Name: URL=http://ocsp.digisign.ro/ocsp
Basic Constraints	Subject Type=CA Path Length Constraint=0
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbrint algorithm	sha1
Thumbrint	8f c3 82 bc 63 b4 86 0c 97 99 86 1e c8 75 6f cf 7a 07 4f 50

7.2. CRL profiles

Certificate Revocation List (CRL) consists of three fields. The first field (tbscertList) contains information about revoked certificates, the second and the third field - signatureAlgorithm and signatureValue contain information about respectively: the identifier of the algorithm used for list signing, and electronic signature of the Certification Authority.

The field of tbscertList is the sequence of mandatory and optional fields. Mandatory fields identify CRL issuer, while optional fields contain information about revoked certificates and CRL extensions. The following fields are the mandatory and optional fields of a CRL:

- **Version**: CRL format version
- **Signature**: contains identifier of the algorithm used by a Certification Authority to sign CRL; DigiSign CAs sign CRLs by means of sha1WithRSAEncryption and sha2WithRSAEncryption algorithm
- **Issuer**: name of the Certification Authority issuing CRL; each DigiSign CA issues its own Certificate Revocation List
- **ThisUpdate**: CRL publication date
- **NextUpdate**: announcement of the date of the next CRL publication; if the field is present, its value describes the maximum date for CRL update.
- **Revokedcertificates**: the list of revoked certificates (the field is empty in the case of lack of revoked certificates); the information consists of three sub-fields: *usercertificates* – serial number of a revoked certificate;
  revocationDate – date of the certificate revocation;
  crlEntryExtensions – contains additional information about revoked certificates – optional.

- **crlExtensions**: extended information about Certificate Revocation List (optional field). Among numerous extensions, the most important are the following ones:
  AuthorityKeyIdentifier - allowing identification of a public key corresponding to a private key used for list signing;
  cRLNumber - containing monotonically increased serial number of the lists issued by a Certification Authority (by means of this extension, a subject is able to define when a specific CRL replaced another list).

Function and meaning of CRLs extensions are the same as for certificate extensions. CRL entry extensions supported by DigiSign may contain the following filed: **ReasonCode** which is the code of the reason for revocation and is a non-critical field. The following reasons of certificate revocation are allowed:

a. **unspecified** – not specified;
b. **keyCompromise** – key compromising;
c. **cACompromise** – Certification Authority key compromising;
d. **affiliationChanged** – subject's data modification;
e. **superseded** – certificate renewal;
f. **cessationOfOperation** – cessation of certificate usage;
g. **certificateHold** – certificate suspension;
h. **removeFromCRL** – certificate removal from CRL.

Revoked certificates are kept for a period of 15 years. Revoked certificates are taken out from the certificate revocation list upon their expiry.

7.3. OCSP profiles

The protocol of on-line certificate status verification (OCSP) allows certificate status evaluation. OCSP service is provided by DigiSign on behalf of all affiliated Certification Authorities. OCSP server, which issues certificate status confirmations, employs a special key pair, generated exclusively for this purpose.

OCSP server certificate has to contain the extension extKeyUsage, described in RFC 3280.
This extension should be set as non-critical, and means that a Certification Authority issuing the certificate to the OCSP server confirms with its signature delegation of the authorization to issue certificate status conformation (of this authority's Subscribers). As well, OCSP server certificate contains the OCSPNoCheck extension, described by RFC 6960. This extension must be declared non-critical which means that an OCSP client receives a response signed with the private key associated to this certificate can trust the OCSP server certificate status, without being necessary to check its revocation status.

The entity receiving a confirmation issued by the OCSP server must support the standard response format with **id-pkix-ocsp-basic** identifier. When the OCSP answer contains an error code (message), the answer is not digitally signed (RCF 6960).

7.3.1. Version number

OCSP server operating within DigiSign issues certificate status confirmations in accordance with the RFC 6960. The only allowable value of the version number is 0 (it is an equivalent of v1 version).

7.3.2. Certificate status information

Information about certificate status is included in certStatus field of SingleResponse structure. This may have one of the following three main values:

a. **GOOD** – indicates the valid status of certificate
b. **REVOKED** – indicates that the certificate was issued and revoked or the certificate was not issued in accordance with the RFC 6960
c. **UNKNOWN** – indicates that there is not enough information to determine the certificate status

7.3.3. Supported standard extensions

In compliance with RFC 6960, DigiSign OCSP server accepts the following extension: **None** – binding a request and a response to prevent reply attacks. Nonce is included in requestExtension of the OCSPRequest and repeated in the field responseExtension of the OCSPResponse.

8. Compliance audit and other assessments

This chapter describes audits intend to control the consistency of DigiSign's actions and of its delegated entities, with the statements and procedures, such as the Certification Policies and the Certification Practice Statements.

DigiSign's audits are carried out by internal terms (internal audit) or by an independent organization/auditor (external audit).

For the provision of qualified electronic certificates and qualified time stamps, DigiSign carries out a qualification audit performed by an accredited Conformity Assessment Body.

8.1. Frequency and circumstances of assessment

The internal audit occurs at least once a year and the external audit occurs on request, at least once at two years.

On-demand audits may be carried out at DigiSign's discretion, at the request of the Supervisory Body as defined in EU Regulation 910/2014, or whenever there is a major change in the service provision process.

8.2. Identity and qualifications of assessor

The internal audit is carried out by the Quality and Audit Department of DigiSign, while the external audit is carried out by an independent organization/auditor.

All assessors that audits DigiSign must act with rigor in order to ensure that policies, statements and services are properly implemented and to detect the non-compliance items which might jeopardize the security of the service. DigiSign commits itself to only hire assessors with high level of expertise in system security, particularly in the field of the audited component.

The audit services regarding the provision of qualified services, are to be performed by independent, recognized, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and are experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies. The audit regarding the provision of qualified services is being carried out by an accredited Conformity Assessment Body, in accordance with the requirements laid out in eIDAS.

8.3. Assessor's relationship to the assessed entity

The assessors for the external audit and the Conformity Assessment Report are appointed by DigiSign with the remark that they all are independent from DigiSign.

The auditor and the CA under audit, must not have any other relationship that would impair the auditor's independence and objectivity. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

8.4. Topics covered by assessment

All audits within DigiSign domain are carried out in compliance with the international accepted rules and regulations, and concern without being limited to:

- DigiSign's physical security,
- procedures of solicitor's identity validation,
- certification services and procedures of service delivery,
- security of software applications and network access,
- security of DigiSign's personnel,
- event journals and procedures for system monitoring,
- data archiving and restoration,
- business continuity plans and disaster recovery plans,
- records concerning the modification of configuration parameters for DigiSign,
- records concerning verifications and analysis carried out for software applications and hardware devices.

8.5. Actions taken as a result of a deficiancy

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by DigiSign with input from the auditors. DigiSign at its sole discretion will determine an appropriate course of action and time frame to rectify the deficiency.

For the provision of qualified electronic certificates and time stamps, in accordance with the European and Romanian law, the course of action and time frame for rectification of any deficiency as set by the Romanian Supervisory Body, must be followed.

8.6. Communication of audit's results

The audit results, in particular the Conformity Assessment Report is made available to DigiSign's Management and to the Romanian Supervisory Body in charge with the accreditation of DigiSign as a Qualified Trust Service Provider.

9. Other business and legal matters

9.1. Fees

The certification services fees and the types of services for which there are charged fees are published on DigiSign's official website. Payments shall be done cash, by payment order, and also bank cards along with the invoice in compliance with the legal provisions in force.

9.1.1. Revocation or Status Information Access Fees

The certificate revocation services, the certificate publication in CRL, or the access to the CRL's published in the Repository (or in other locations) are free of charge. DigiSign can settle fees for certificate status verification services by means of OCSP protocol or other systems.

9.1.2. Fees for other services

DigiSign can charge fees for other services rendered, such as:

- Generating keys for Certification Authorities or Subscribers,
- Testing of applications and including them in the list of recommended applications,
- Selling licenses,
- Design, implementation and installation activities,
- Sale of CPS, of Certification policy, handbooks, guides etc.
- Training courses.

9.1.3. Refund Policy

DigiSign offers a refund to Subscribers in accordance with the refund policy published on DigiSign's official website. Subscribers who choose to invoke the refund policy should have all issued certificates revoked.

9.2. Financial responsibility

DigiSign will cover damages it might cause due to the provision of the certification services for persons that build their conduct on the legal effects of qualified certificates up to the 10.000 euros for every risk insured. The insured risk represents every damage caused even if there are more than one, following to DigiSign not fulfilling the liabilities mentioned by law.

9.3. Confidentiality of business information

All DigiSign's information was gathered, stored and processed in accordance with the requirements of Regulation (EU) No. 910/2014 and in compliance with the internal provisions of Regulation No. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and other provisions of Union common law on data protection.
Relations between a Subscriber, a Relying Party and DigiSign are based on trust.

A third party might have access only to information public available in certificates. Other data delivered in applications sent to DigiSign will not be willingly disclosed to a third party under any circumstance (except the legal situations).

A party will be exonerated from the liability of disclosing confidential data if:

a. the information was known to the contracting party before it was received by the other contracting party; or
b. the information was disclosed after obtaining the written consent of the other party; or
c. the party was legally forced to disclose the information.

Disclosing any information to the parties involved in fulfilling the obligations will be confidentially done and will extend only to that information necessary to fulfill the obligations.

9.3.1. Type of information considered confidential/private

DigiSign, its employees and also the entities that perform certification activities are committed to keep the information secret both during and after employment. There are considered private and confidential information:

- Information provided by Subscribers which are not part of the public key of the certificates
- Documents supplied by/to Subscribers (e.g. contracts, offers, agreements etc)
- Records of system transaction (all types of transactions, as well as data for transactions' control, the so called system transactions logs);
- Record of events (logs) connected with certification services, kept by DigiSign,
- Results of internal and external audits, if they are a threat for DigiSign's security,
- Emergency plans,
- Information about steps taken to protect the hardware devices and software applications, information about management of the certification services and planned registration rules.

9.3.2. Type of information not considered confidential/private

All information required for certification services' proper functioning are not considered confidential or private. In particularly concerns information included in a certificate by the issuing Certification Authorities and the information published at www.digisign.ro. A Subscriber that applies for obtaining a certificate is aware of the type of information included in the certificate and agrees with their publishing.

Part of the information provided by or to the Subscriber might be made available to other entities only with the written consent of the Subscriber and for the stated purpose in the contract concluded with the Subscriber.

The following information categories are available for the public in the Repository:

- Policies and practices regarding the provision of trust services
- The pricelist for services provided,
- Guides for users,
- CA Certificates,
- Subscriber's certificates (after obtaining their approval),
- Certificates Revocation List (CRL), etc.

9.3.3. Disclosure of certificate revocation reason

If a certificate was revoked upon the request of an authorized party (not the party whose certificate is being revoked), information about the revocation and the related reasons are disclosed to both parties.

9.3.4. Disclosure of non-public information to law enforcement officials

As a general principle, no document or record belonging to DigiSign is released to law enforcement agencies or officials except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to DigiSign to be under appeal when served on DigiSign (DigiSign being under no obligation to determine this).

9.4. Protection of personal information

DigiSign ensures that the confidentiality and integrity of registration data is protected, especially when exchanged with the Subscriber and the Subject or between DigiSign's distributed system components,

in accordance with the requirements of Regulation (EU) No. 910/2014 and in compliance with the internal provisions of Regulation No. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and other provisions of Union common law on data protection.
The purpose of personal data processing is to provide certification services.

9.4.1 The personal data protection assurance plan

DigiSign, as a provider of qualified trust services, acts as a personal data operator according to art. 4 paragraph 7 of Regulation no. 679/2016.
DigiSign implements the security measures required by Regulation (EU) no. 910/2014, Regulation no. 679/2016 and by the supervisory authority in the field of personal data processing, to guarantee that:
• appropriate technical and organizational measures are taken to ensure the security of the processed data, to protect the rights of the Subjects and to comply with the principles provided by Regulation no. 679/2016 and the provisions of Regulation (EU) no. 910/2014;
• access to DigiSign services refers to the processing of only those identification data that are adequate, relevant and not excessive to grant access to that service
• the confidentiality and integrity of the registration data is ensured.

9.4.2 Information considered as personal data

All information about the Subject that leads to its identification are considered as personal data.

9.4.3 Responsibility to protect personal data

DigiSign and its employees are committed to maintaining the confidentiality of information with personal character both during the provision of certification services and after termination the validity of the certificates.
DigiSign will not disclose personal information to any third party, for any reason, with the exception of situations in which it will be obliged to do so by law or by the authorities competent.

9.4.4 Notification of data subjects and their consent for the use of personal data

In the process of issuing a digital certificate, the Subjects/Beneficiaries are informed about the need to use their personal data, in order to provide the service, and the need to grant consent. Lack of consent entails the impossibility of providing the service.
Also, the Subjects/Beneficiaries have the possibility to explicitly opt for the use of personal data for other purposes expressly communicated by DigiSign by contract or otherwise.

9.4.5 Disclosure as a result of an administrative or legal process

DigiSign is exonerated from liability for the disclosure of personal data of the Subjects/Beneficiaries in the following situations:
• towards the Supervisory Body according to the applicable legislation;
• towards the institutions and authorized bodies, based on the public law obligations that DigiSign has, in accordance with the legal provisions;

9.4.6 Other Circumstances for Disclosure

The following situations constitute exceptions to the obligation to preserve the confidentiality of personal data that exonerate DigiSign from liability:
a. disclosure of personal information to:
• auditors within the audits to which DigiSign is subject according to the provisions of Regulation (EU) no. 910/2014 under conditions of confidentiality;
• third parties who base their conduct on the certification services provided by DigiSign in the relationship with which the Subject uses the certificate
• the courier companies with which DigiSign has a contract, with the consent of the Subject/Beneficiary, if he has opted for the transmission of the certificate to his home address or to another communicated address, respecting the same obligations regarding the security of personal data that it also has DigiSign;
• proxies to whom DigiSign has outsourced certain services;
b. the personal information that appears in the certificates or in the public Directories (Depository), with the consent of the Subject/Beneficiary;
c. in any other justified situations with prior notification of the Subject/Beneficiary.

9.5. Intellectual property rights

All trademarks, patents, brand marks, licenses, graphic images etc. used by DigiSign are and will be the intellectual property of their legal owners. DigiSign commits itself to mention this thing according to requests imposed by owners.

All trademarks, patents, brand marks, licenses, graphic images etc., belonging to DigiSign are and remain its property, no matter if they are along with patents, utility models, copyright or not and cannot be reproduced or delivered to a third party without the previous agreement in writing of DigiSign.

Every key pair associated to a certificate issued by DigiSign is the property of the subject of the certificate, described in the field *Subject* of the certificate, except the certificates where the Subscriber (legal entity) is different from the Subject, in which case the owner is a legal entity.

9.6. Responsibilities and warranties

A. Certification Authorities
All electronic certificates issued by DigiSign are compliant with X.509 V3 standard, thus DigiSign undertakes the obligation to ensure such compliance. Moreover, DigiSign guarantees that all the requirements set out in the appropriate CPS, indicated in the Certificate under the Cerificate Policy field, are complied with.

The essential guarantee provided by DigiSign is that the procedure used are in accordance with the rules declared in the applicable CP and CPS (e.g. for EU qualified electronic certificates, this CPS shall be applied). Other responsibilities may be set out in the Terms and Conditions and in the Agreement signed with the Subscriber.

Unless otherwise expressly provided in this CPS or in the applicable legislation, DigiSign disclaims all warranties and obligations of any type, especially regarding the negligence and lack of reasonable care on the part of the Subscribers, Subjects and Relying Parties.

B. Registration Authorities

The Registration Authorities within DigiSign domain have the obligation to comply with the applicable CPS and with all relevant internal procedures.

C. Subscribers and/or Subjects
The Subject has the obligation to accept the Terms and Conditions relevant to the service requested. If the Subject does not comply with the Terms and Conditions, DigiSign can not provide the service.

By accepting the Terms and Conditions, the Subject agrees with the appropriate Certification Practice Statement and Certification Policy, and thus with his/hers responsibilities, liabilities and obligations as provided in the previously mentioned documents.

The main liability of a Subject refers to the one that he/she has towards Relying Parties for any use that is made of his/hers QSCD (including private keys, electronic certificates), unless the Subject can prove that he/she has taken all necessary measures for a timely revocation (if the case).

D. Relying Parties
The Relying Parties have the following obligations and responsibilities, without limitation:

- Thoroughly verify every electronic signature from a certificate or document received. To check the signature the Relying Party must:
  - specify the certification path that contains every certificate of the Certification Authorities that make possible the verification of the signature from the signer's certificate,
  - make sure that the chosen certification path is the best for creating the signature; in some cases it is possible to exist more than a path starting from a given certificate (by means of which the signature was created) and to a Certification Authority on which the signature verification is based.
  - make sure that none of the certificates from the certification path, belonging to DigiSign, is not on the revoked or suspended certificate lists;
  - check if all the certificates from the certification path belong to a Certification Authority and these are authorized to sign other certificates,
  - (optionally) specify the date and time when a document or a message was signed. This thing is possible only if the document or message was time stamped (before its signing) with a time stamp issued by a Time Stamp Authority, or a time stamp was associated with an electronic signature just after the document's signing; such a verification allows the implementation of non-repudiation services or can be used to solve disputes,
  - verify, using a defined certification path, the credibility of the signer's certificate, document or message and the authenticity of the signature;
- carry out accurately the cryptographic operations using software applications and devices with a security level corresponding to the sensitivity level of certificates processed and the credibility level of the used certificates;
- consider an electronic signature as being invalid if by means of applied software and devices is not possible to determine if the electronic signature is valid or if the verification result is negative;

- electronic signature verification aims at stating whether: (1) an electronic signature was created by means of a private key corresponding to a public key from a certificate issued by DigiSign for a Subscriber and (2) the message (document) signed was not modified after signing.

- trust only those certificates of public keys that:
  - are used in compliance with the stated purpose and correspond to the applicability areas mentioned by the Relying Party, for example, by a signature policy,

  - whose status was verified based on corresponding Certificate Revocation Lists or by means of DigiSign's OCSP service;

- specify the conditions that must be fulfilled by a public key certificate and an electronic signature in order to be considered valid; these conditions may be formulated, for example, as a certification policy accepted and then published.

9.7. Limitations of liability

DigiSign is not liable for (a) the damages caused by force majeure and/or unforeseeable circumstances (acts of God), (b) the damages caused by the inappropriate use of the qualified trust services, (c) the damages caused by the storage of erroneous data in DigiSign's databases and their inclusion in the certificates issued for the Subject, in case the Subject declared that those data are correct, (d) the damages caused by the theft or the deterioration of the devices used to store the certificates, the unauthorized or improper use of them or any negligence of the Subject regarding their storage and use.

9.8. Indemnities

DigiSign assumes no financial responsibility for improperly used certificates, CRLs or any other services provided by DigiSign.

9.9. Term and termination

This CPS remains in force until notice of the opposite is communicated by DigiSign on its Repository at the official website. Notified changes are appropriately marked by an indicated version and or edition. The CPS is reviewed at least once a year.

9.10. Individual notices and communications with participants

All notices, major changes and other communications which may or are required to be given, served or sent pursuant to this CPS, shall be in writing and shall either be published at www.digisign.ro. Individual notice may be made as follows:

- registered mail, return receipt requested,
- an express courier service,
- hand delivery,
- electronic mail, signed with a qualified electronic signature and/or seal, if necessary.

9.11. Dispute resolution procedures

The contracting parties will try to resolve any disputes amicably. Requests will be sent to the email address office@digisign.ro, and the response to requests will be made within a maximum of 30 days.

Any dispute that cannot be resolved amicably will be addressed to the competent courts in Bucharest.

9.12. Governing law

DigiSign provides qualified digital certificates and electronic seals services in accordance with the European and Romanian applicable law:

- Regulation EU 910/2014 (eIDAS);
- Applicable national legislation.

9.13. Compliance with applicable law

The qualified trust services DigiSign provides are compliant with eIDAS Regulation, as well as with relevant applicable Romanian legislation.
The compliance with the applicable law is certified by the accreditation of DigiSign as a Qualified Trust Service Provider, issued by Romanian Supervisory Body.