Certification Policy

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:	**2**
Approved by:	**General Manager**	Version:	**3**

OID: **1.3.6.1.4.1.34285.1.1.1.1.2.1.0**

DIGISIGN S.A.

74B Nicolae G. Caranfil, 1st District

014146, Bucharest, Romania

+4 031 620 20 00

+4 031 620 20 80

office@digisign.ro

www.digisign.ro

Str. Nicolae G. Caranfil nr. 74B, Sector 1, 014146, București
Tel.: 031 620 2000 | Fax: 031 620 2080 | office@digisign.ro

Document history

Edition	Version	Description	Date	Author
1	0	First release: Certification Policy 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	Remote signature with QSCD-R	December 03, 2018	Policies and Procedures Management Body
1	3	Minor updates	July 28, 2020	Policies and Procedures Management Body
2	0	Minor updates	December 22, 2022	Policies and Procedures Management Body
2	1	Minor updates	February 19, 2024	Policies and Procedures Management Body
2	2	Minor updates	October 24, 2024	Policies and Procedures Management Body
2	3	Address update	December 21, 2024	Policies and Procedures Management Body

Str. Nicolae G. Caranfil nr. 74B, Sector 1, 014146, București
Tel.: 031 620 2000 | Fax: 031 620 2080 | office@digisign.ro

Contents

1. Introduction

A Certification Policy (hereinafter CP) is 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 this CP is to establish what a participant within DigiSign PKI must do and the applicability of a certificate according to its type. The rules and principles stated in this document determines the level of security and assurance provided by a specific type of certificate.

1.1. Overview

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.

This document describes the general rules and principles followed by DigiSign as a Qualified Trust Service Provider (QTSP), in order to successfully issue, renew, suspend, revoke, validate and generally administrate digital certificates, in accordance with the legal requirements relating, namely:

- ✓ EU Regulation no. 910/2014 (hereinafter named eIDAS), on electronic identification and trust services for electronic transactions in the internal market and all subsequent regulations and directives
- ✓ National applicable legislation in force

1.2. 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.

While a CA ensures the proper management of certificates and carries out, in some cases, the liability, the end users – Subject, Subscribers and Relying Parties - have the responsability to use those certificates according to the policy of each type of certificate. The certificate policies have also a major impact on the relying party responsabilities, as those carrie out the liability regarding which type of certificate they trust.

DigiSign issues certificates for any applicant, within the legal previsions and as long as they comply with DigiSign Certificate Practice Statement and Certification Policy.

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).

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.

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.

All entities which take action within the certification process – RAs, CAs, VAs – and final users – Subjects and Relying Parties – are presented in detail, in legal, commercial and technical terms, in DigiSign Certification Practice Statement.

1.3. Policy name and identification

The official name of this document is DigiSign CP. This document outlines the rules and principles which applies for each type of certificate issued by DigiSign's CAs. This document applies to all entities participating in or using digital certificates issued by DigiSign's CAs.

This document describes the general rules and principles used to comply with Regulation (EU) no. 910/2014 and national applicable legislation, in order for DigiSign's Authorities to provide trust services to end users, such as Qualified Electronic Signatures, Qualified Electronic Seals. A detailed description of the practice and procedures used by DigiSign's Authorities to provide trust services are described in DigiSign Certification Practice Statement (hereinafter CPS).

2. Type of certificates

An electronic certificate is a suite of information and attributes that binds the signing and verification data to an entity and which confirms its identity.

A certificate for electronic signature means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. A qualified certificate for electronic signature represents a certificate for electronic signature that is issued by a QTSP and meets the requirements laid down in Annex 1 of eIDAS Regulation.

A certificate for electronic seal means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person. A qualified certificates for electronic seal represent a certificate for electronic seal that is issued by a QTSP and meets the requirements laid down in Annex IIII of eIDAS Regulation.

Thus, DigiSign, as a QTSP, issues the following types of qualified certificates to natural and legal persons, with a high level of assurance.

Certification Authority	Certificate type	Subject type	QC Statement	LoA	Guarantees and financial obligations
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificate	Natural person	qc-n	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificate with pseudonym	Natural person	qc-n	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates issued on a QSCD	Natural person	qc-n-qscd	high	Full
Policy identifier (OID number):					

1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates with a pseudonym issued on a QSCD	Natural person	qc-n-qscd	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates issued on a QSCD and hosted by DigiSign for remote-signature	Natural person	qc-n-qscd-r	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates	Legal person	qc-l	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates issued on a QSCD	Legal person	qc-l-qscd	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates issued on a QSCD and hosted by DigiSign for remote-seal	Legal person	qc-l-qscd-r	high	Full
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.1.3					
DigiSign Qualified CA Class 3 2017	Qualified Electronic Certificates for other Authorities	Authorities within DigiSign PKI		high	Full

The qualified certificates are issued by DigiSign Qualified CA Class 3 2017 with a high level of assurance. The qualified certificates are intended for the creation and verification of Qualified Electronic Signatures and Qualified Electronic Seals, according to eIDAS. The qualified electronic certificates

issued by DigiSign determines with high precision the identity of a subject, the authenticity of an organization or the credibility of an Authority.

In this case, the registration process is made by completing a form which requires information about the identity of the applicant. Apart from verifying the domain which hosts the e-mail address, the Registration Authority (RA) checks if the documents are in their validity period and if they are suitable. For qualified certificates, there are specific identity documents allowed for identification: Identity Card, Passport, Resident Certificate and Fiscal Registration Certificate (eg: the birth certificate is not a valid identity document allowed for identification). All information requested and provided are subject to rigorous verification by the RA within DigiSign domain.

Moreover, for qualified certificates, the subject or the subject's authorized representative has to present himself in person to a DigiSign Registration Authority, according to the procedures stated in DigiSign CPS, in order to be properly identified with his/her original valid identity documents. The identity of applicants (natural persons) can also be verified through remote video identification with video support that allow verification of the security elements for the identity documents presented and offer the DigiSign operator the possibility to verify and validate the correspondence between the natural person and the documents.

Qualified Electronic Certificates (hereinafter QEC) issued by DigiSign can be used to create and validate qualified electronic signatures with the same legal effect as the handwritten ones. QEC ensures who the subject is and the non-repudiation of the signed document.

The certificates issued by DigiSign Qualified CA Class 3 2017 for other authorities within DigiSign PKI are mainly intended for the Validation Authority and the Time-Stamping Authority (hereinafter qTSA).

For the qualified electronic certificates, DigiSign offers full guarantees liability, as described in DigSign CPS.

3. Services

DigiSign, as a Qualified Trust Service Provider, offers trust services within its PKI and in addition to those, some services such as: registration, verification, issuance, renewal, publication, suspension, revocation, management, time-stamping, repository, implementantion, schooling etc. Each service has a defined set of rules and procedures, described in DigiSign CPS and further summarized in this CP.

a. Registration: refers to the registration of the applicant and implies the verification and authentication of the subject's identity, including by remote video identification procedure.
b. Issuance: refers to the effective issuance of the certificate by one of DigiSign CAs, after the registration process has been successfully conducted.
c. Renewal: refers to the issuance of another certificate by the same DigiSign CA which issued the first certificate, and to the same user. Depending on the method of renewal, some information about the subject may be changed (eg: address or telephone number).
d. Publication: refers to the storage and publication of the certificate, which always happens after the holder's certificate acceptance; the storage is made in the electronic register of certificates, managed by DigiSign and permanently accessible at www.digisign.ro, which is the main source of information for all participants within DigiSgn PKI.
e. Suspension: refers to the temporary and reversible revocation of the certificate.
f. Revocation: refers to the validity cancellation of the certificate and the withdrawal of any rights of use.

g. Validation: refers to the validation of a certificate either through the OCSP service (offers real time information about the certificate status), either through the Certificate Revocation Lists (offers once at 24 hours information about the certificate status, namely if that particular certificate is revoked or not), either through the electronic register of the issued certificate.
h. Time-Stamping: refers to an additional service offered by DigiSign's Time-Stamping Authorities, which confirms the existence of some electronic data, in a particular form, at an exact moment of time.

4. Prices

The trust services provided by DigiSign are commercially available. The prices for these services depend on the nature and complexity of the service required. The prices for each service are published on DigiSign's official website www.digisign.ro.

DigiSign reserves the right to charge extra fees for any additional service, such as implementation, training, consulting etc, but only if those are subject to an agreement between the parties.

5. Amendments

DigiSign CP is administrated by DIGISIGN S.A. through the CPS Management Body, complying with the provisions laid out in chapter 1.4 of DigiSign CPS.

6. Other information

Privacy Policy

DigiSign has implemented a privacy policy which complies with DigiSign CPS. The privacy policy is publicly available and can be accessed at www.digisign.ro.

Publication and Information

DigiSign's trust services and repository are accessible through several means of communication, such as:

- on the web: www.digisign.ro
- by email: office@digisign.ro
- by post: 74B Nicolae G. Caranfil street, 1st District, 014146, Bucharest, Romania

In general, DigiSign's official website – www.digisign.ro – will be used to make any type of notification and communication. Other means of individual notices and communication is specified in relevant service-based Policy and/or Practice Statement.

Availability

DigiSign ensures the following opening hours: from Monday to Friday, 9 AM to 5 PM, with the exception of Romanian legal holidays and also makes available to the public the Support Department on a 24x7 basis at suport@digisign.ro and +4 031 620 20 00, for any information regarding the trust services it provides, as well as for the additional products and services in its offer.

DigiSign ensures the access to its headquarters from 74B Nicolae G. Caranfil street, 1st District, 014146, Bucharest, Romania, for people with disabilities by providing a special parking lot, access ramp and an elevator with displays of audio and visual directions. Furthermore, DigiSign provides tools for magnifying and suitable contrast on its website www.digisign.ro.