
# CertDigital Certification Services Policy

| **ISSUED BY :** | | |
|---|---|---|
| **DEPARTAMENT** | **NAME** | **DATE** |
| ELECTRONIC SERVICES COMPARTMENT | COMPARTMENT CHIEF | 19.03.2011 |

| **APPROVED BY :** | | |
|---|---|---|
| **DEPARTMENT** | **NAME** | **DATE** |
| MANAGEMENT OF POLICIES AND PROCEDURES | Electronic Services Manager | 01.06.2016 |

| **HISTORY OF MODIFIERS :** | | | |
|---|---|---|---|
| **VERSION** | **AUTHOR** | **DETAILS OF MODIFICATIONS** | **DATE:** |
| 1.0.0 | COMPARTMENT CHIEF | Publication of the first version | 19.03.2011 |
| 1.0.1 | **Technical Director** | Adding new certification authorities<br>CertDigital Qualified CA Class 3 G2<br>CertDigital Enterprise CA Class 3 G2<br>CertDigital NonRepudiation CA Class 4 G2 | 01.06.2016 |
| 1.1 | Electronic Services Manager | Revision and alignment to the requirements of European Regulation no. 910/2014 | 19.04.2017 |

# Cuprins

# 1. Introduction

## 1.1. CertDigital brand

CertDigital is the registered trademark under which S.C. Centrul de Calcul S.A. Provides certification and time-stamping services. Every time CertDigital refers to the content of this document, those references involve the S.C. Centrul de Calcul S.A.

## 1.2. Content

CertDigital Certification Policy (CP) describes the rules and general principles applied by CertDigital in the process of public key certification and use of time stamping authority (TSA) as well as other non-repudiation services.

Certification policy defines:

- ☐ entities involved in certification processes,
- ☐ the responsibilities and obligations of each entity,
- ☐ types of certificates,
- ☐ confirmation types,
- ☐ identity verification procedures
- ☐ scope of applicability.

The detailed description of the above rules is provided in the DPSC Statement of Practice of Certification Services (DPSC) and respectiv In the Declaration of Practice of Time Stamping Services (DPSMT).

Knowing the Certification Services Policy and the Certification Services Practice Statement is of particular relevance to CertDigital's subscribers and partner entities.

## 2. The Certificates

The certificate is a data string (message) that contains at least the name and authority, identifier, subscriber identifier, public key, validity period, serial number and signature of the issuing authority.

Certificates are used to link the subscriber's personal data to specific public keys.

The owner of the certificate is also the owner of the private key, corresponding to the public key contained in the certificate. The identification data contained in the certificate allows other parties to accurately determine the owner of the certificate. If the private key is used during the electronic signing of a message, the recipient of the message can be certain that the message was created using the private key corresponding to the public key contained in the certificate (so it was created by the owner of the certificate) and the message has not been changed by someone else.

CertDigital Certification Authority CA confirms by issuing a certificate for a subscriber:

- ☐ Its identity or the credibility of other data, such as the address of the mailbox;
- ☐ The public key contained in the certificate belongs to that subscriber.

Because of the above, partner entities, after receiving a signed message, can determine who owns the certificate that signed the message and, he may optionally hold him accountable for his actions or commitments

CertDigital provides services in accordance with the legislation and practices in the field. Certification authority keys are protected using security hardware modules (Hardware Security Module - HSM), certified according to FIPS 140-1 and FIPS 140-2 level 3. CertDigital implements physical and procedural system controls.

CertDigital Certification Authority issues certificates of different Classes, with different levels of credibility. The credibility of the certificate depends on the process of checking the identity of the subscriber and the effort made by CertDigital operators to verify the data sent by the applicant in his application for registration. The certificate class may also depend on the Security class of the server or network device for which the certificate is issued. CertDigital specialists can verify a subscriber's technical status and security class of a subscriber before issuing a certificate of the highest Credibility Class.

CertDigital Certification Authority CA issues certificates to the general public and provides services specific to a public key infrastructure. Among the most important functions of the certificates issued by CertDigital CA are included (but not limited to):

- ☐ Signing of electronic documents,
- ☐ Electronic seals
- ☐ Securing e-mail messages,
- ☐ Securing Web transactions,
- ☐ Securing network communications
- ☐ Applying code signing,
- ☐ Stamping time

## 2.1 Class 1 certificates

Class 1 certificates are issued by the Certification Authority Cert Digital Simple CA and **CertDigital Simple CA G2**. These certificates are only designed for internal purposes and uses and does not provide any guarantee of the identity of the subject. Simple certificates are primarily intended to test the performance of applications or devices before purchasing final certificates. Certification Authority Cert Digital Simple CA and CertDigital Simple CA G2 issues certificates for almost all purposes. In most cases, during the registration process, the address

of the electronic mailbox and / or the name and surname of the natural person or of the legal entity's representative are being verified.

Class 1 certificates contain the following policy identifier:

**{CertDigital}[1]id-policy(1) id-cp(1)id-Class-1(1)**

CertDigital assumes no financial obligation and does not provide any warranty for certificates (and their content) issued under the above policy.

## 2.2 Class 2 certificates

Class 2 certificates are issued by the Certification Authority Cert Digital Organization CA Class 2 and **CertDigital Organization CA Class 2 G2**. These are personal certificates and are primarily intended to secure electronic mail or authenticate customers during online sessions. Operators of Certification Authorities Cert Digital Organization CA Class 2 and CertDigital Organization CA Class 2 G2 checks data provided by customers during the certification process. The identity of the requesting natural person or the representative of the legal person is subject to a detailed check. The authenticity of the e-mail box address included in the certificate is also verified.

Class 2 certificates contain the following policy identifier:

**{CertDigital}.id-policy(1).id-cp(1).id-Class-2(2)**

Certificates issued under this policy offer limited guarantees and responsibilities.

## 2.3 Class 3 certificates

Class 3 certificates are issued by 2 Certification Authorities: **CertDigital Enterprise CA Class 3 G2,** and **CertDigital Qualified CA Class 3 G2**.

Certificates issued in this class can be Qualified or Certified Certificates for securing binary objects and protecting data transmissions using the IPSec, SSL,

[1] {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital's IANNA assigned number (47898)

and TLS protocols. CertDigital operators verify the data provided by customers (organizations or institutions) during the registration process. All data to be included in the certificate is verified.

Based on a certificate issued by CertDigital Enterprise CA Class 3 G2 or CertDigital Qualified CA Class 3 G2, you can accurately determine the identity of a subject or the authenticity of an organization.

Qualified Certificates issued by CertDigital Qualified CA Class 3 G2 can be used to create electronic signatures to replace handwritten signatures.

**Qualified certificates** are issued by the Certification Authorities Cert **CertDigital Qualified CA Class 3 G2**. These certificates are compliant with European Parliament Directive 1999/93 / EC on the Community Electronic Signature Framework, Electronic Signature Law 455/2001 from Romania and Government Decision 1259 / December 2001 on the Rules for the Application of the Electronic Signature Law.

Certification Authorities **CertDigital Enterprise CA Class 3 G2** and **CertDigital Qualified CA Class 3 G2** use a certificate issued with the algorithm sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

Class 3 certificates contain the following policy identifier:

**{CertDigital} id-policy(1) id-cp(1)id-Class-3(3)**

In addition, for the Qualified Certificates, the policy identifier is added**itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1),** for certificates issued by **CertDigital Enterprise CA Class 3 G2** add the policy identifier **{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2)**

CertDigital's financial responsibility for data from certificates issued under the above policy is outlined in the Statement of Certification Services Practices

(DPSC). Certificates issued under this policy provide full guarantees and responsibilities

## 2.4 Class 4 certificates

Class 4 certificates are issued by the Authorities CertDigital Non-Repudiation CA Class 4 G2. These certificates are primarily intended for subordinate Certification Authorities or other trusted service providers (OCSP or Authorities for Time stamping). CertDigital Non-Repudiation CA Class 4 G2 operators Verifies the identity of customers who have to appear personally at one of CertDigita's counters. We will verify the empowerment of the firm, the authenticity and the correctness of the provided identity documents as well as the acts of the organization. CertDigital Non-Repudiation CA Class 4 G2 also accepts authenticated documents by a notary. Based on a certificate issued by CertDigital Non-Repudiation CA Class 4 G2, it is possible to determine exactly the identity of a subject, the authenticity of an organization or the credibility of an external Certification Authority. Subscriber keys that hold a Class 4 certificate must be protected using hardware security modules (HSMs)

Class 4 certificates contain the following policy identifier:

**{CertDigital} id-policy(1) id-cp(1)id-Class-4(4)**

Certificates issued under this policy provide full guarantees and responsibilities.

CertDigital Subscriber can choose the type of certificate according to its needs. The types of certificates are described in detail in the Statement of Certification Services Practices (DPSC) which can be consulted on the CertDigital Web site. This information can also be received by e-mail by sending a message to: office@certdigital.ro.

# 3. Non-repudiation tokens

Non-repudiation tokens are data structures (messages) containing at least:

- ☐ Information provided by the customer (eg, hash value, serial number of the certificate, application number, etc.) to a non-repudiation authority and
- ☐ The electronic signature of the respective authority

Non-repudiating authorities offering customer service are affiliated with CertDigital. By issuing a token, a non-repudiation authority confirms the occurrence of an event at the moment of its creation or at a prior time. This event can be: submitting a document, signing date, etc.

The partner entity can verify, based on the received data, the accuracy of the signature based on trust in CertDigital CA G2.

## 3.1 The time stamps

Timestamps are issued by Cert Digital Time Stamping Authority and CertDigital Time stamping Authority G2. Time stamps, as a basic element in ensuring non-repudiation, are issued both to private individuals and those belonging to an organization.

- ☐ Time-stamps can be incorporated into: Electronic signatures,
- ☐ Acceptance of electronic transactions,
- ☐ Data archiving,
- ☐ Notarization of electronic documents etc.

The rules governing the operation of the Temporary Marking Authority as well as other additional information related to this system are described in a separate document (See the General Policy of Temporal Marking).

The time stamp token contains the following policy identifier:

**{CertDigital}[2].id-Time-Stamping(2).Id-Policy(1)**

CertDigital's financial responsibility for the time, date and other additional information included in the time stamps issued under the above policy is set out in the Statement of Practice of Time Tracking Services. Cert Digital Time Stamping Authority and CertDigital Time stamping Authority G2 provides warranties for time stamps issued within the limits specified in Statement of Practice of Time Stamping Services.

### 3.2 OCSP Confirmation Response

OCSP (Online Certificate Status Protocol) responses are issued by the **CertDigital Validation Authority G2**. OCSP responses are primarily used to determine the status of certificates. These services are publicly available and represent an alternative to Revocable Certificate Lists. CertDigital Validation Authority G2 provides warranties for OCSP issued responses within the limits described in the CPP. The way the OCSP authority works and additional information on this service is presented on the web page (see http://www.certdigital.ro) and in Statement of Certification Services Practices.

## 4. Guarantees offered by CertDigital

Depending on the type of certificate issued, CertDigital guarantees that it will make the effort necessary to properly check the information included in the certificates (See the Statement of Certification Services Practices - Chapter 2.1.1: Obligations).

Verification of information is important first of all for partner entities receiving messages from a subscriber who is identified by a qualified digital certificate issued by CertDigital. Consequently, CertDigital is financially responsible for damages resulting from the negligence or errors committed by CertDigital in respect to these types of certificates. CertDigital's responsibilities depend on the

[2] {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital's IANNA assigned number (47898)

subscriber's certificate class, and the responsibility lies with both the subscriber and the partner entities that trust the information in the certificate (See the Statement of Certification Services Practices)

CertDigital's warranties may be limited by certain restrictions. These restrictions are brought to the attention of the subscriber who confirms this in a statement (See the Certificate Acceptance Statement). CertDigital guarantees the uniqueness of electronic signatures for its subscribers.

## 5. Acceptance of the certificate

CertDigital's responsibilities and warranties apply from the time the subscriber accepts the certificate. How to provide the certificate and accept the certificate are described in the Code of Practice and Procedures (see Chapter 3.5 Acceptance of the Certificate) and are detailed in the agreements concluded with the subscribers.

## 6. Certification Service

CertDigital certification service provides four basic services:

I. registration

II. issuing a digital certificate,

III. renewing a certificate,

IV. revoke a certificate and

V. verifying the status of a certificate

VI. Issuing an electronic seal

VII. renewing an electronic seal

VIII. revoke an electronic seal and

V. verifying the status of an electronic seal

CertDigital also offers the following non-repudiation services:

I. Authority for Temporary Stamping,

II. On-line validation of digital certificate status.

II. On-line validation of electronic seal.

The registration is designed to verify the identity of a subscriber and precedes the issuance of the certificate (See the Statement of Certification Services Practices, Chapter 3.1 Requesting a Certificate and Chapter 3.2 Issuing the Digital Certificate).

Renewal of a certificate occurs when a registered subscriber already wishes to obtain a certificate for the same public key with the change of the period of validity (See the Statement of Certification Services Practices, Chapter 3.7 Extending the Validity of a Valid Certificate).

Revocation of a certificate occurs when the private key corresponding to the public key in the digital certificate has been compromised or is suspected of being compromised (See Statement of Certification Services Practices, Chapter 3.6 Revocation of a Certificate).

Checking the status of a certificate is a service through which CertDigital confirms the validity of a digital certificate using the CRLs issued by affiliated authorities. Verification of the status of a certificate can also be accomplished through online certificate status validation service (see the Statement of Certification Services Practices).

CertDigital allows each pair of keys (private-public) to be generated by the subscriber. CertDigital can make recommendations about key generation devices. Under certain specific conditions, CertDigital can generate unique key pairs and deliver these keys to subscribers.

## 7. Partner entity

The partner entity is required to properly check each electronic signature on the received documents (including the digital certificate). During the verification process, the partner entity must use the procedures and resources provided by CertDigital. They specify, among other things, that the list of revoked certificates published by CertDigital and the permitted certification paths (see the statement of Certification Services Practices, Chapter 1.4.2 Registration Authority).

Each document for which digital signature verification issues are to be found must be rejected and must be verified by other means or procedures, eg verification of a document by a notary.

## 8. Subscriber

The subscriber is required to safely keep his private key in order to prevent unauthorized access to a third party. If there is a suspicion that it was accessed by a third party, the subscriber is obliged to immediately notify the authority that issued his/her digital certificate. The information provided to the authority must be sufficient to determine precisely the identity of the person to whom the digital certificate will be revoked.

## 9. Update your certification policy

These changes will be available to all subscribers through the CertDigital Web site. Subscribers who do not accept the changes to the certification policy should send CertDigital a statement to this effect and waive the services provided by CertDigital.

## 10. Taxes

Certification services provided by CertDigital are commercially available. Tariffs for these services depend on the class of certificates issued or held by a subscriber and the type of service requested. Prices are shown in the price lists available on the CertDigital site (http://www.certdigital.ro).