Certification Policy
certSIGN

Version 1.7

Date: 31 January 2019

Document history

Version	Date	Reason	The person who made the change
1.0	April 2006	Releasing the first version	Electronic Services Manager
1.1	July 2009	Changing the company's registered office to 107A Oltenitei Rd., District 4, Bucharest, Romania.	Electronic Services Manager
1.2	March 2014	Adding the new CA Class 3 Enterprise G2	Technical Director
1.3	July 2015	Adding the new certification authorities: certSIGN CA Class 2 G2 certSIGN Qualified CA Class 3 G2 certSIGN Non-Repudiation CA Class 4 G2	Technical Director
1.4	10 January 2016	Adding the new closed circuit certification authorities, that issue certificates for the Electronic Payment System operated by Transfond S.A.	Technical Director
1.5	25 January 2016	Adding a new certification authority designed for issuing code signing certificates. The OID for Non-EV Code Signing 2.23.140.1.4.1. was introduced in the description of the certification policy. Also, the OV 2.23.140.1.2.2. OID was included in the certification policy associated to SSL certificates.	Technical Director
1.6	26 November 2018	Update change headquarters	PKI Policies Manager
1.7	31 January 2019	Annual review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
Electronic Services Manager	Electronic Services Manager	27 January 2006

Distribution list

Destination	Distribution date
Public-Internet	25 January 2016

This document was approved by

Version	Name	Data
1.0	Policies and Procedures Management Body	April 2006
1.1	Policies and Procedures Management Body	June 2009
1.2	Policies and Procedures Management Body	March 2014
1.3	Policies and Procedures Management Body	June 2015
1.4	Policies and Procedures Management Body	December 2015
1.5.	Policies and Procedures Management Body	January 2016
1.6.	Policies and Procedures Management Body	November 2016
1.7.	Policies and Procedures Management Body	January 2019

Content

1. Introduction

certSIGN's Certification Policy (CP) describes the general rules and principles applied by certSIGN during the certification process of the public keys and in using the time stamping authority (TSA), as well as for other non-repudiation services. The certification policy defines:

- The entities involved within the certification process,
- The responsibilities and obligations of every entity,
- The types of certificates,
- The types of confirmations,
- The identity checking procedures and
- Applicability area.

The detailed description of the above mentioned rules is presented in the **Certificate Practices Statement (CPS**).

The knowledge of the Certification Policy, as well as of the CPS is important especially for the users and for the certSIGN's partner entities.

2. Certificates

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

The certificates are used to link the subscriber's personal data with the specific public keys. The certificate's owner is also the owner of the private key corresponding with the certificate's public key. The identification data contained in the certificate allow other parties to determine the exact owner of the certificate. If the private key is used during the electronic signing of a message the receiver can be sure that the message was created using the private key corresponding with the certificate's public key (otherwise said it was created by the certificate's owner) and the message was not modified by anybody else.

By issuing a certificate to a subscriber the certSIGN CA Certification Authority confirms:

- His identity or the credibility of other data, such as the electronic mail address;
- The public key contained in the certificate belongs to the respective subscriber.

Due to those mentioned above, the partner entities, after receiving a signed message, can determine who the certificate's owner is that signed the message, and optionally, can make him liable for his actions or assumed engagements.

certSIGN provides services in compliance with the legislation and the relevant practices. The certification authority's keys are protected using hardware security modules (HSM), certified according with FIPS 140-1 level 3. certSIGN implements the physic and procedural checking of the system.

The certSIGN Certification Authority issues certificates of different Classes with different credibility levels. The certificate's credibility depends on the procedure regarding the subscriber's identity checking and on the effort made by certSIGN's operators to check the data sent by the solicitant within his registration request. As well, the certificate's class can depend on the security Class of the server or of the network device for which the certificate is issued. certSIGN's experts can check the technical status and the security Class of one subscriber's IT system before issuing a certificate with the highest credibility Class.

The Certification Authority certSIGN CA issues certificates for the large audience and provides services specific for a public key infrastructure. Among the most important applications of the certificates issued by certSIGN CA there can be mentioned (without limiting to):

- Electronic documents signing,
- Security for the e-mail messages (electronic mail),
- Security for Web transactions,
- Security for network communications,
- Signature for applications' code,
- Time stamps.

2.1. Class 1 certificates

The class 1 certificates are issued by the Certification Authority **certSIGN Demo CA Class 1.** These certificates are used only for demonstrations and do not provide any warranty regarding the subject's identity. The demo certificates are mainly for testing the applications' or devices' performances before buying the final certificates. The Certification Authority certSIGN Demo CA Class 1 issues certificates for almost every purpose. In most cases during the registration process the e-mail address and/or the name and first name of the natural person or the legal entity's representative are checked.

The class 1 certificates contain the following policy identifier:

{certSIGN}* id-policy(1) id-cp(1)id-Class-1(1)

certSIGN does not assume any financial obligation and does not offer any warranty for the certificates (and their content) issued under the above mentioned policy.

2.2. Class 2 certificates

The Class 2 certificates are issued by the **certSIGN CA Class 2** and **certSIGN CA Class 2 G2** Certification Authorities**.** These are personal certificates and are mainly used for securing electronic correspondence or for clients' authentication during online sessions. The operators of the certSIGN CA Class 2 and certSIGN CA Class 2 G2 Certification Authorities check the data provided by clients during the certification process. The identity of the natural person solicitant or of the legal entity's representative is checked in detail. The authenticity of the e-mail address included in the certificate is also checked.

The Class 2 certificates contain the following policy identifier:

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

The certificates issued under this policy provide limited warranties and responsibilities.

Additionally, class 2 certificates are issued with 3 closed circuit certification authorities. These certificates are issued for the Electronic Payment System (EPS) operated by Transfond S.A., based on a technical protocol. The authorities that issue certificates for EPS are:

1. CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.2
2. CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.1
3. CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.3

The class 2 certificates for EPS refer the following policy identifier:

{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2).id-Transfond(1)

The certificates issued under this policy must respect the technical protocol concluded between certSIGN and Transfond.

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (20715)

2.3. Class 3 certificates

The Class 3 certificates are issued by the **certSIGN Qualified CA Class 3**, **certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3**, **certSIGN Enterprise CA Class 3 G2** and **certSIGN Code Signing CA Class 3 G2** Certification Authorities. The certificates issued within this class can be qualified certificates or certificates for securing the binary objects and the protection of data transmissions using IPSec, SSL and TLS protocols. The certSIGN operators check the data provided by the clients (organizations or institutions) during the registration process. All data that are going to be included in the certificate are thoroughly checked. Based on a certificate issued by certSIGN Qualified CA Class 3, certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3, certSIGN Enterprise CA Class 3 G2 and **certSIGN Code Signing CA Class 3 G2** an individual's identity or an organization's authenticity can accurately be determined.

The qualified certificates issued by certSIGN Qualified CA Class 3 and certSIGN Qualified CA Class 3 G2 can be used to create electronic signatures to replace the holograph signatures.

The qualified certificates are issued by the **certSIGN Qualified CA Class 3** and **certSIGN Qualified CA Class 3 G2** Certification Authorities. These certificates are compliant with Directive 1999/93/EC of the European Parliament regarding the Communitarian Framework related to the Electronic Signature, the Electronic Signature Law 455/2001 in Romania and the Government Decision 1259/December 2001 regarding the Electronic Signature Law Applicability Terms.

certSIGN Qualified CA Class 3 and certSIGN Enterprise CA Class 3 Certification Authorities use a certificate issued with the sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) algorithm, while certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3 G2 and **certSIGN Code Signing CA Class 3 G2** use a certificate issued with the sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) algorithm.

The Class 3 Certificates contain the following policy identifier:

{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)

In addition, for 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 the certificates issued by **certSIGN Enterprise CA Class 3 G2**, the policy identifier is added

{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)

and for the certificates issued **certSIGN Code Signing CA Class 3 G2**, the policy identifier is added

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4)code-signing(1)} (2.23.140.1.4.1)

certSIGN's financial responsibility for the data in the certificates issued under the above policy is described in the CPS (CPP) (see http://www.certSIGN.ro/repository). The certificates issued under this policy provide complete warranties and responsibilities.

Additionally, class 3 certificates are issued with a closed circuit certification authority. The certificates are issued for the Electronic Payment System (EPS) operated by Transfond S.A., based on a technical protocol. The authority that issues certificates for EPS are:

1. CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.3.1.1

The class 3 certificates for SEP refer the following policy identifier:

{certSIGN} .id-policy(1). id-cp(1).id-Class-3(3).id-Transfond(1)

The certificates issued under this policy must respect the technical protocol concluded between certSIGN and Transfond. The certificates issued by this authority do not include the qualified certificate identifier.

2.4. Class 4 certificates

The Class 4 certificates are issued by the **certSIGN Non-Repudiation CA Class 4** and **certSIGN Non-Repudiation CA Class 4 G2** Certification Authorities. These certificates are mainly for the subordinated Certification Authorities or other trust services providers (OCSP or Time Stamp Authorities). The certSIGN Non-Repudiation CA Class 4 and **certSIGN Non-Repudiation CA Class 4 G2** operators check the identity of the clients that must present themselves at one of the certSIGN's counters. The power of attorney from the company, the authenticity and correctness of the identity documents as well as the organization's documents

will be checked. certSIGN Non-Repudiation CA Class 4 and **certSIGN Non-Repudiation CA Class 4 G2** also accept documents certified by a public notary. Based on a certificate issued by certSIGN Non-Repudiation CA Class 4 or **certSIGN Non-Repudiation CA Class 4 G2** an individual's identity, an organization's authenticity or the credibility of an external Certification Authority can accurately be determined. The availability period for a Class 4 certificate is of minimum 2 years. The keys of the subscriber that owns a Class 4 certificate must be protected using hardware security modules (HSM).

The Class 4 certificates contain the following policy identifier:

{certSIGN} id-policy(1) id-cp(1)id-Class-4(4)

The certificates issued under this policy provide complete warranties and responsibilities.

The certSIGN Subscriber can choose the type of certificate fit for his needs. The certificate types are described in detail within the CPS (CPP) that can be read on certSIGN's Web site. As well, this information can be received by electronic mail after sending a message to the address: office@certSIGN.ro.

3. Non-repudiation counters

The non-repudiation counters are data structures (messages) containing at least:

- The information provided to (for example hash value, serial number of the certificate, request number etc.) a non-repudiation authority and
- The electronic signature of the respective authority.

The non-repudiation authorities that provide services to the clients are affiliated to certSIGN.

By issuing a counter a non-repudiation authority confirms the appearance of an event when it is created or at a previous moment. This event can be: sending a document, the date when the signature was created etc. The partner entity can check, based on the received data, the signature's correctness based on the trust in certSIGN CA.

3.1. Time Stamps

The time stamps are issued by the **certSIGN Time-Stamping Authority**. The time stamps as basic element to insure the non-repudiation are issued both to private persons and to those from an organization. The time stamps can be incorporated in:

- Electronic signatures,
- Electronic transactions acceptance,
- Data archiving,
- Electronic document notarizing etc.

The rules that settle the operating way of the Time Stamp Authority as well as other additional information related to this system are described in a separate document (see the certSIGN Time-Stamping Authority Policy).

The time stamp counter contains the following policy identifier:

{certSIGN}*.id-Time-Stamping(2).Id-Policy(1)

The certSIGN financial responsibility for the time, date and other additional information included in the time stamps issued under the above policy is described in certSIGN Time-Stamping Authority Policy (please see http://www.certSIGN.ro/repository). certSIGN Time-Stamping Authority provides warranties for time stamps issued within the limits mentioned in certSIGN Time-Stamping Authority Policy.

3.2. OCSP Confirmation Response

OCSP responses (*Online Certificate Status Protocol*) are issued by the **certSIGN Validation Service** Authority. The OCSP responses are used mainly to determine the certificate's status. These services are public available and represent an alternative for the Certificate Revocation Lists (CRL). certSIGN Validation Service provides warranties for the OCSP responses issued, within the limits described in the CPS. The way in which the OCSP authority functions and the additional information regarding this service are presented on the web page (please see http://www.certSIGN.ro) and in the CPS.

4. Warranties provided by certSIGN

Depending on the type of certificate issued, certSIGN warranties that will make the necessary effort to check properly the information included in the certificates (please see the CPS - Chapter 2.1: Obligations). The information checking is important in first instance for the partner entities that receive messages from a subscriber that identifies himself through a qualified digital certificate issued by certSIGN. Therefore, certSIGN is responsible from financial point of view

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (25017)

for the damages resulted following the negligence or the errors made by certSIGN regarding these types of certificates. certSIGN's responsibilities depend on the subscriber's certificate class and the responsibility is both towards the subscriber and to the partner entities that trust the information in the certificate (please see the CPS – Chapter 2.2 Liability and 2.3 Financial Liability).

The certSIGN warranties can be limited by certain restrictions. These restrictions are announced to the subscriber that confirms this thing within a statement (please see the statement for Certificate Acceptance). certSIGN warrants the uniqueness of its subscribers' electronic signatures.

5. Certificate acceptance

certSIGN's responsibilities and warranties are applicable from the moment the subscriber accepts the certificate. The way the certificate is delivered and its acceptance are described within the CPS (please see chapter 4.4 Certificate Acceptance) and are detailed within the agreements concluded with the subscribers.

6. Certification service

certSIGN provides four basic services:

(1) registration,

(2) issuing a digital certificate,

(3) renewal of a certificate,

(4) revocation of a certificate and

(5) checking the status of a certificate.

Moreover, certSIGN also provides non-repudiation services:

(6) Time Stamp Authority,

(7) On-line status validation service for digital certificates.

The purpose of the registration is to check a subscriber's identity and precedes the operation of issuing the certificate (please see the CPS, chapter 4.1 Sending the request and Chapter 4.3 Certificate issuance).

The renewal of a certificate takes place when a subscriber already registered wants to obtain a certificate for the same public key with the modification of the availability period (please see the CPS, Chapter 4.7 Key Certification).

The revocation of a certificate takes place when the corresponding private key from the digital certificate was compromised or is susceptible of being compromised (please see the CPS, Chapter 4.10 Certificate Revocation).

The checking of a certificate's status is a service through which certSIGN confirms the validation of a digital certificate using the Certificate Revocation Lists (CRL) issued by the affiliated authorities. The checking of a certificate's status can be done by means of the on-line validation service for the certificate status (please see the CPS, Chapter 4.10.7 On-line Certificate Status Verification).

certSIGN allows that every key pair (private-public) should be generated by the subscriber. certSIGN can make recommendations regarding the devices for key generation. In certain specific conditions, certSIGN can generate unique key pairs and deliver them to the subscribers.

7. The partner entity

It is mandatory for the partner entity to check every electronic signature on the received documents (including the digital certificate). During the checking process the partner entity must use the procedures and resources made available by certSIGN. Among others these specify the need to check the certificate revocation list published by certSIGN and the allowed certification ways (please see the CPS, Chapter 2.1.4 Relying Parties' Obligations).
Every document for which there are problems when checking the digital signature must be rejected and checked using other ways or procedures, such as the document's checking by a public notary.

8. The subscriber

It is mandatory for the subscriber to safely keep his/her private key to prevent the unauthorized access of a third party to it. In case there is the suspicion that the private key was accessed by a third party, the subscriber must immediately inform the authority that issued the respective digital certificate. The information sent to the authority must be detailed enough so as to allow determining the exact identity of the person whose digital certificate will be revoked.

9. Updating the certification policy

certSIGN's certification policy can be periodically modified. These modifications will be available to all subscribers via certSIGN's Web site. The subscribers who do not accept the modifications brought to the certification policy must send certSIGN a statement in this regard and to renounce the services provided by certSIGN.

10. Taxes

The certification services provided by certSIGN are commercially available. The prices for these services depend on the class of the certificates issued to or owned by a subscriber and on the type of the requested service. The taxes are described in the price lists available on certSIGN's Web site (http://www.certSIGN.ro).