multicert
Engineering for digital security

# MULTICERT Root CA Certification Practices Statement

Policy

MULTICERT_PJ.ECRAIZ_24.1.1_0001_en.doc

**Identification of the Project:** ECRaiz da MULTICERT

**Identification of the CA:** MULTICERT Root CA

**Rating:** Public

**Version:** 3.0

**Date:** 07/10/2015

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edificio 3, Piso 3 – 2740-266 Porto Salvo, Oeiras, Portugal
Phone: +351 217 123 010 Fax: +351 217 123 011

**Document Identifier:** MULTICERT_PJ.ECRAIZ_24.1.1_0001_en.doc

**Key Words:** DPC

**Document Typology:** Policy

**Title:** MULTICERT Root CA Certification Practices Statement

**Original Language:** Portuguese

**Publication Language:** English

**Access Level:** Public

**Date:** 07/10/2015

**Current Version:** 3.0

**Identification of the Project:** ECRaiz da MULTICERT

**Identification of the CA:** MULTICERT Root CA

**Client:** ---

**Version History**

| Version Nr. | Date | Details | Author(s) |
|---|---|---|---|
| 1.0 | 21/03/2014 | Approved version | MULTICERT S.A. |
| 2.0 | 07/07/2014 | Approved version – Inclusion of CabForum Compliance | MULTICERT S.A. |
| 3.0 | 07/10/2015 | Approved version – Mozilla Policy Compliance and CabFroum Revision | MULTICERT S.A. |

**Related Documents**

| Document ID | Details | Author(s) |
|---|---|---|
| MULTICERT_PJ.ECRaiz_24.1.2_0001_pt.pdf | Certificate Policy of MULTICERT Root CA | MULTICERT S.A. |
| MULTICERT_PJ.ECRaiz_24.1.13_0001_pt.pdf | Principle Disclosure Statement | MULTICERT S.A. |

# Summary

# 1 Introduction

## Purposes of the Document

The purpose of this document is to define the procedures and practices done by MULTICERT during the performance of its digital certification activity in the scope of the Root CA from MULTICERT. This document is referred to as being the Certification Practices Statement (CPS) by the Root CA from MULTICERT.

## Target Public

This document shall be publicly available and is aimed to all entities which are related in some way to the Root CA from MULTICERT.

## Document Structure

This document follows the structure defined and proposed by the PKIX Working group from IETF, in document RFC 3647[1], also according to the structure recommended by ETSI TS 102 042[2].

The first ten chapters are dedicated to describing the most important procedures and practices in the scope of the digital certification by the Root Certification Authority from MULTICERT. Chapter 11 describes the legal subjects.

[1] *cf.* RFC 3647. 2003, Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

[2] *cf. ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, v2.4.1*

# 2 General Context

This document is a Certification Practices Statement, hereinafter referred to as CPS, which purpose is the definition of a set of practices for the issuing and validation of Certificates, and for the assurance of reliability. It is not meant to name legal rules or obligations, but to inform. Therefore, it is intended that this document should be simple, straightforward, and understood by a wide public, including people with no technical or legal knowledge.

This document describes the general practices for the issuing and management of the Certificates followed by the Root Certification Authority from MULTICERT (MULTICERT Root CA), and explains what a Certificate provides, as well as how the procedures should be followed by Relying Parties and by any other interested person, to trust in the Certificates issued by MULTICERT Root CA. This document may undergo regular updates.

## 2.1 Overview

The practices for the creation, signature, and issuing of Certificates, as well as the revocation of invalid certificates, performed by a Certification Authority (CA) are fundamental to ensure the reliability and trust of a Public Key Infrastructure (*PKI*).

This CPS specifically applies to MULTICERT Root CA, and acknowledges and implements the following standards:

- RFC 3647: *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003*;
- RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile, 2008*;
- *ETSI TS 101 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,v2.4.1 and;*
- *CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.3.0.*

MULTICERT Root CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

## 2.2 Designation and Identification of the Document

This document is the Certification Practices Statement from MULTICERT Root CA. The CPS is represented in a certificate by a unique number called "object identifier" (OID). The value of the OID associated with this document is 1.3.6.1.4.1.25070.1.1.1.0.7.

This document is identified by the data in the following table:

| DOCUMENT INFORMATION | |
|---|---|
| **Document Version** | Version 3.0 |
| **Document State** | Approved |
| **OID** | 1.3.6.1.4.1.25070.1.1.1.0.7 |
| **Issuing Date** | September 2015 |
| **Validity** | 1 year |
| **Location** | https://pki.multicert.com/index.html |

## 2.3 Participants in the Public Key Infrastructure

### 2.3.1 Certification Authorities

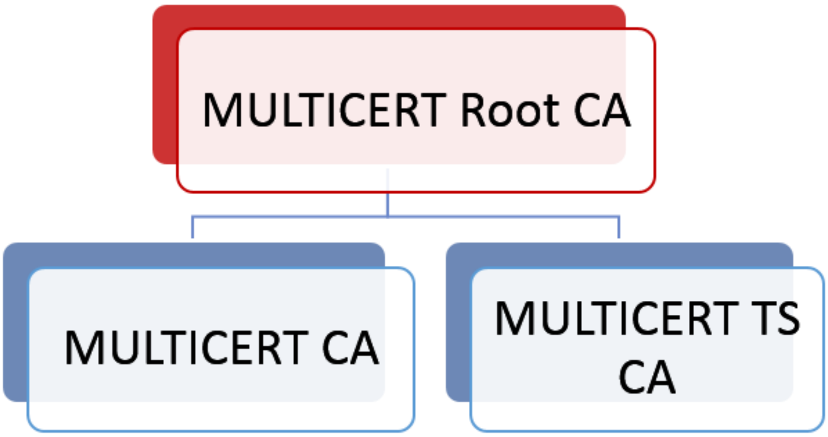
MULTICERT, as the Managing Entity of MULTICERT's PKI, meets the provisions laid down in the standards and applicable legislation, and assumes the competences therein, being responsible for providing services and assuring the procedures (even subcontracting third parties) that may ensure the functionalities described next:

1. Creation of the cryptographic key pairs associated with each of the Certification Authorities;
2. Reception and validation of the requests for the issuing of Certificates made by the subordinate Certification Authorities (CAs), as well as the rest of the subscribers;
3. Issuing of certificates related to the requests for certificates, which are consistent with the format required by the Certification Authority from MULTICERT;
4. Reception and validation of the requests for the suspension, reactivation and revocation of certificates;
5. Publication of the certificates (when, where, and if appropriate) and information regarding its state;
6. Assuring the continuous availability of the public information to all its users;

MULTICERT currently holds three Certification Authorities:

- MULTICERT Root Certification Authority (MULTICERT Root CA);

- MULTICERT Certification Authority (MULTICERT CA);
- MULTICERT Trust Services Certification Authority (MULTICERT TS CA).



### 2.3.1.1 MULTICERT Root Certification Authority (MULTICERT Root CA)

MULTICERT Root CA is a Certification Authority accredited by the National Security Authority according to ETSI 102 042, and is therefore able to issue certificates for Subordinate Certification Authorities.

MULTICERT Root CA is included in several recognition programs for Root Certification Authorities which make the MULTICERT Root CA recognized in several *browsers* and systems, thus promoting its global spread.

| CERTIFICATE INFORMATION | |
|---|---|
| **Distinct Name** | CN=MULTICERT Root Certification Authority, O=MULTICERT, Serviços de Certificação Electrónica S.A., C=PT |
| **Signature Algorithm** | sha256RSA |
| **Serial Number** | 6e e9 1e f8 b2 d5 c9 ac |
| **Validity Period** | 13/03/2014 to 13/07/2039 |
| **Digital Mark** | c5 81 41 59 a9 64 74 73 e8 71 07 2a e5 32 8d 2d 9d 90 d6 9e |

### 2.3.1.2 MULTICERT Certification Authority (MULTICERT CA)

MULTICERT CA is a Certification Authority accredited by the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx ), with accreditation number ANS-ECC-7/2014, at the date 20/06/2014, as foreseen in the Portuguese and European legislation, and is therefore legally capable to issue all types of digital certificates, including qualified digital certificates (digital certificates with the highest security level foreseen in the legislation). It falls within two hierarchies of trust:

- Own self-assigned hierarchy of trust, for independence purposes regarding other hierarchies of trust;
- International hierarchy of trust with WebTrust accreditation (http://www.webtrust.org/) and is present in the majority of the operating systems and Web browsers.

This way, MULTICERT CA is known in the majority of the operating systems and *browsers*, and its main role is to manage the certification services: issuing, operation, suspension, revocation for its subscribers.

MULTICERT CA issues certificates of:

- Qualified Signature for natural person;
- Qualified Signature of Quality
- Qualified Signature for the representation of collective person;
- Authentication for natural and collective person
- Advanced Signature for natural and collective person;
- SSL Certificates for web server;
- Application Certificates;
- Services from PKI MULTICERT, i.e., certificates for the required services under the scope of MULTICERT PKI:
  - OCSP online validation.

| **CERTIFICATE INFORMATION** | |
|---|---|
| **Distinct Name** | CN=MULTICERT Entidade de Certificação 001, OU = Accredited Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT |
| **Signature Algorithm** | Sha1RSA |
| **Serial Number** | 07 27 8e f0 |
| **Validity Period** | 29/05/2020 |
| **Digital Mark** | ef 2e 98 f4 42 ee cd 10 b9 8f 2a da 72 16 09 8c e4 83 53 18 |

| **CERTIFICATE INFORMATION** | |
|---|---|
| **Distinct Name** | CN=MULTICERT Certification Authority 002, OU = Accredited Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT |
| **Signature Algorithm** | Sha256RSA |
| **Serial Number** | 17 33 10 19 7f 6e 01 c1 |
| **Validity Period** | 13/03/2014 to 12/07/2025 |
| **Digital Mark** | 02 a7 f8 8d c1 76 71 e7 a6 93 82 b3 26 4e f2 1e 5d b9 3b 4e |

#### 2.3.1.3 MULTICERT Trust Services Certification Authority (MULTICERT TS CA)

MULTICERT TS CA is a Certification Authority accredited by the National Security Authority (http://www.gns.gov.pt/gns) as foreseen in the Portuguese and European legislation. It falls within two hierarchies of trust:

- Own self-assigned hierarchy of trust, for independence purposes regarding other hierarchies of trust;
- International hierarchy of trust with WebTrust accreditation (http://www.webtrust.org/) and is present in the majority of the operating systems and Web browsers.

This way, MULTICERT TS CA is known in the majority of the operating systems and web browsers, and its main role is to manage the certification services: issuing, operation, suspension, revocation for its subscribers.

MULTICERT TS CA issues certificates of,

- Code Signing;
- Object Signing;
- Services from PKI MULTICERT, i.e., certificates for the required services under the scope of PKI MULTICERT:
    - Timestamping;
    - TSL (Trust Service Status List).

| **CERTIFICATE INFORMATION** | |
|---|---|
| **Distinct Name** | CN=MULTICERT Trust Services Certification Authority 001, OU=MULTICERT Trust Services Provider, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT |
| **Signature Algorithm** | Sha256RSA |
| **Serial Number** | 64 f5 57 61 cc 29 0e 51 |
| **Validity Period** | 14/03/2014 to 13/07/2025 |
| **Digital Mark** | 59 9e 95 f8 93 e0 67 91 2e 87 65 bf 4c dd f1 e8 1e 94 96 40 |

### 2.3.2 Registration Authority

The Registration Authority (RA) is the entity authorized to collect and check the identity information from subordinate CAs and the information required by MULTICERT for each type of certificate to be issued. MULTICERT may act as RA and/or establish agreements with other entities in order for these to perform this role.

## 2.3.3 Other participants

### 2.3.3.1 Accreditation Authority

The Accreditation Authority is a competent entity for the accreditation and supervision of the Certification Authorities.

In general, the role of the Accreditation Authority, in Portugal performed by the National Security Authority (ANS), is related to compliance audit/inspection in order to assess if the processes used by the CAs in its certification activities are compliant with the minimum requirements established by Portuguese and European legislation, as well as with the terms of this CPS.

The Accreditation Authority is one of the "parties" that contributes to the trust of the Qualified Certificates due to the competences that carries over the issuing CAs. In the scope of its duties, the Accreditation Authority performs the following roles regarding the CAs:

a) Accreditation: procedure to approve the CA to perform its activity based on an evaluation of parameters as diverse as physical safety, *hardware* and *software*, access and operation procedures;

b) Supervision: procedure based on the inspections made to the Certification Authorities to regularly check the compliance parameters;

c) Security Auditor required figure independent of the CA's circle of influence.

### 2.3.3.2 Security Auditor

Figure independent of the Certification Authorities circle of influence, and required by the Accreditation Authority. It's mission is to audit the Certification Authorities infrastructure regarding the equipment's, human resources, processes, policies and rules, and the submission of an annual report to the Accreditation Authority. For the list of Security Auditors from Certification Authorities accredited by the Accreditation Entity, please see http://www.gns.gov.pt/media/3992/ListagemdeAS.pdf.

# 2.4 Certificate Use

The certificates issued in the PKI domain from MULTICERT are used by the different subscribers, systems, applications, mechanisms and protocols with the purpose to ensure the following security services:

a) Access control;
b) Confidentiality;
c) Integrity;
d) Authentication, and
e) Non-repudiation.

These services are obtained by resorting to the use of public key cryptography, through its use in the trust structure provided by MULTICERT's PKI. Therefore, the identification, authentication, integrity and non-repudiation services are obtained by using digital signatures. Confidentiality is guaranteed through recourse to cryptographic algorithms, along with mechanisms to establish and distribute keys.

### 2.4.1 Appropriate Use

The requirements and rules defined within this document apply to all the certificates issued by MULTICERT Root CA.

The certificates issued for technological equipment are aimed to be used in authentication services and in establishing cryptographic channels.

The certificates issued for the purpose of being used by confidentiality services, issued based on the rules defined herein, may be used to process information classified up to the CONFIDENTIAL degree, when used over public networks (e.g. Internet). In its use within proprietary networks, the classification degree of information shall be defined by the national organism responsible within the scope of treatment of classified information/matters.

The certificates issued in MULTICERT's PKI are also used by the Trusting Parties for the verification of the chain of trust of a certificate issued within MULTICERT's PKI hierarchy, as well as to ensure the authenticity and identity of the issuer of a digital signature created by the private key corresponding to the public key held in a certificate issued under MULTICERT's PKI.

### 2.4.2 Non-Authorised Use

Certificates can be used in other contexts only to the extent of what is allowed by the applicable legislation.

The certificates issued in MULTICERT's PKI cannot be used for any other purpose outside the scope of the uses previously described.

Certification services offered by MULTICERT's PKI that were not designed nor authorised to be used in high risk activities or which require an activity exempt from failures, such as those related with the operations of hospital facilities, nuclear and air traffic control, and railway traffic control facilities, as well as any other activity where a failure can lead to death, personal injury or serious damages to the environment.

## 2.5 Policy Management

### 2.5.1 Entity responsible for document management

The management of this Certification Practices Statement is the responsibility of the Authentication Working Group of MULTICERT's PKI.

### 2.5.2 Contact

| **NAME** | Authentication Working Group |
|---|---|
| **Address:** | MULTICERT S.A.<br>Lagoas Park, Edificio 3, Piso 3<br>2740-266 Porto Salvo, Oeiras, Portugal |
| **E-mail:** | pki.documentacao@multicert.com |
| **Internet:** | www.multicert.com |
| **Phone:** | +351 217 123 010 |
| **Fax:** | +351 217 123 011 |

### 2.5.3 Entity responsible for determining the compliance of the CPS regarding the Policy

The Authentication Working Group determines the compliance and internal application of this CPS (and/or related CPs), and submits it to the Management Group for approval.

### 2.5.4 Procedures for Approving the CPS

The validation of this CPS (and/or related CPs) and following corrections (or updates) shall be carried out by the Authentication Working Group. Corrections (or updates) shall be published as new versions of this CPS (and/or related CPs), replacing any CPS (and/or related CPs) previously defined.

The Authentication Working Group shall also determine when the changes in the CPS (and/or related CPs) lead to a change in the object identifiers (OID) of the CPS (and/or related CPs).

After the validation phase, the CPS (and/or related CPs) is submitted to the Management Group, which is the entity responsible for the approval and authorization of the changes made on this type of documents.

# 3 Publishing and Storage Responsibility

MULTICERT reserves the right to publish information related to digital certificates it issues in a repository available *online*, as well as to publish information about the status of the certificate in third party repositories.

MULTICERT maintains a document repository *online* where it releases information about its practices, procedures, and content of certain policies, including the CPS.

All parties associated to the issuing, use or management of MULTICERT's certificates are hereby notified that MULTICERT may publish submitted information in its repository, which is publicly accessible, in order to provide information about the status of the digital certificate.

MULTICERT refrains from making publicly available certain elements of documents related with security controls, procedures, internal security policies, etc. However, these elements are subject to formal accreditation audits, as the ETSI TS 102 042.

## 3.1 Repositories

MULTICERT S.A. is responsible for the repository functions of the Root CA from MULTICERT, publishing, amongst others, information related to the practices adopted and the status of the issued certificates (CRL).

The technological platform of the repository is configured according to the following indicators and metrics:

- Minimum 99,990% of answers to requests for obtaining the CRL;
- Minimum 99,990% of answers to requests for the CPS document;
- Maximum number of requests for CRL: 50 requests/minute;
- Maximum number of requests for CPS: 50 requests/minute;
- Medium number of requests for CRL: 20 requests/minute;
- Medium number of requests for CPS: 20 requests/minute.

The access to information made available by the repository is made through the HTTPS and HTTP protocol, and the following security mechanisms are implemented:

- The CRL and CPS can only be changed through well defined processes and procedures;
- The technological platform of the repository is properly protected by the most recent techniques of physical and logical security;
- The human resources who manage the platform have the proper training and experience for the service in question.

## 3.2 Publishing of Certification Information

MULTICERT S.A. maintains a repository in a *web* environment, allowing for the Trusting Parties to make *online* researches regarding the revocation and other information regarding the status of the Certificates.

MULTICERT S.A. always makes the following public information available *online*:

- The most recent electronic copy of this CPS and Certificate Policies (CP) from MULTICERT Root CA, digitally signed by a duly authorised individual and with a digital certificate attributed for that purpose:
- CPS from MULTICERT Root CA made available in URI: **https://pki.multicert.com/index.html**
- CP of the self-signed certificate from MULTICERT Root CA made available in URI: **https://pki.multicert.com/index.html**
- CRL from MULTICERT Root CA – URI: **https://pki.multicert.com/index.html**
- Certificate from MULTICERT Root CA – URI:**https://pki.multicert.com/index.html**
- Other relevant information – URI: **https://pki.multicert.com/index.html**

Additionally, all previous versions of the CP and CPS from MULTICERT Root CA will be kept outside of the public free access repository. However, they may be made available when requested, as long as its need is justified.

## 3.3 Periodicity of the Publication

The updates to this CPS and corresponding CP shall be published immediately after its approval by the Management Group, according to section 10.2.

The certificate from MULTICERT Root CA shall be published immediately after its issuing. The CRL shall be published at least, once every 4 months.

## 3.4 Access Control to the Repositories

The information published by MULTICERT S.A. shall be available on the Internet, being subject to access control mechanisms (read-only access). MULTICERT S.A. has implemented physical and logical security measures in order to prevent the addition, deletion, and change of the records in the repository by unauthorized people.

# 4 Identification and Authentication

## 4.1 Attribution of Names

This section describes the procedures used to authenticate the Certification Authorities before the certificates are issued, as well as questions regarding name disputes.

### 4.1.1 Types of Names

MULTICERT ensures the issuing of certificates with one *Distinguished Name* (DN) **X.500**. Issues certificates for the subscribers who submit documentation with a verifiable name.

MULTICERT shall ensure inside its trust infrastructure the non-existence of certificates that, having the same DN, may identify distinct entities.

### 4.1.2 Need for Significant Names

MULTICERT shall ensure that the names used in its issued certificates identify in a significant way its users. This means that it shall be ensured that the used DN is appropriate for the user in question and that the *common name* component of the DN represents the user in a way easily understood by people. However, MULTICERT may issue certificates under pseudonym, as long as they are identified in this way.

### 4.1.3 Interpretation of the Names Formats

The rules for the interpretation of the names are defined in an appropriate document, with the access restricted to people authorized by MULTICERT.

### 4.1.4 Name Uniqueness

MULTICERT shall control the existing names in order to ensure that a certificate has a unique DN, related to only one entity and that it is not ambiguous.

### 4.1.5 Solution of Name Disputes

MULTICERT shall be responsible for the attribution and approval of the DNs, and also for the resolution of any disputes that may arise.

### 4.1.6 Registered Trademark Recognition, Authentication, and Roles

The names issued by MULTICERT shall respect to the maximum the registered trademarks. MULTICERT shall not deliberately allow the use of registered names, whose entity cannot prove that they are its property. However, MULTICERT may refuse to issue certificates with names of registered trademark if it finds another identification to be more convenient.

### 4.1.7 Method for Proving Possession of the Private Key

Whenever MULTICERT is not responsible for generating the pair of cryptographic keys to be attributed to the user, before proceeding with the issuing, MULTICERT shall ensure that the user has a private key corresponding to the public key present in the certificate request.

The method of proof shall necessarily be as more complex as needed according to the important of the requested type of certificate, which is documented in the Certificate Policy of the regarded certificate.

## 4.2 Identity Validation in the Initial Registration

MULTICERT is responsible for the authentication of the identity of the clients candidates for obtaining a certificate. The ways to proceed to this authentication include:

- Ensure that the client exists and that he authorized the issuing of the certificate;
- Ensure that the client is aware, to be integrated in the hierarchy of the Root CA from MULTICERT, he will have to comply with what is established under this document, as indicated in point 4.2.1;
- Ensure that MULTICERT's Root CA legal representatives accepted the client in question inside its hierarchy.

The registration and authentication process shall be ensured by the following: it is the responsibility of the RA to correctly register the final users of the certificate, using the means necessary to positively identify them in a legal way. Among the operations to be performed to reach this objective are:

1. Verify in documents officially acknowledged by the State where the subscriber (individual or organization) is registered:
   a. Full name;
   b. Contact data, including the contact address;
   c. Its legal unique identification.
2. Ensure the physical presence of the subscriber at the moment of the registration, unless there is already a trust relation previously based on that physical presence of the subscriber;

The procedures for the identification and authentication of subscriber previously unknown shall follow the following rules:

1. The subscriber or its legal representative (in case of a collective person) shall present themselves physically to MULTICERT;
2. The physical identification shall be authenticated against identifying proofs that must be compliant with the following provisions:
   a. To be officially recognized in the jurisdiction where the subscriber is registered;
   b. To indicate the full name of the subscriber and its official address;
   c. To have at least one identity proof with a photograph of the subscriber (always applicable);
   d. To indicate a unique registration number inside of the jurisdiction where it was issued.
3. In case of certificates for non-human subscribers, the mentioned authentication processes shall apply to the people who are authorized to request certifications for the specified subscribers.

3. MULTICERT shall verify that each candidate for obtaining a certificate has the right to obtain that certificate and, in case obtaining that certificate also implies obtaining attributes or privileges of any kind, the candidate really has the right to those privileges and attributes;

4. When necessary, MULTICERT shall require the requesting entity of a certificate prepares and submits an appropriate logical request of certificate to the CA;

5. Also when necessary, MULTICERT shall verify the correctness of the information included in the logical request of certificate from the requesting entity.

### 4.2.1 Agreement with the Subscriber

MULTICERT shall keep a record of the agreement signed with the subscriber, including:

1. Agreement of the terms and conditions with the subscriber. In case the subscriber of the certificate is distinct from the subject, the later shall also be informed of the terms and conditions;
2. Consent for the maintenance of the records by MULTICERT, with the information used in the registration, as well as the information of subsequent events regarding the agreement and its object;
3. Permission to pass this information to third parties under certain conditions;
4. Permission to pass information over the status of the issued certificates, under the agreement, to unspecified third parties.

#### 4.2.1.1 Certificate Request

MULTICERT:

1. Shall require that the requesting entity of a certificate prepares and submits the appropriate data to the request, as specified in this CPS;
2. When necessary, shall require that the final requesting entity submits its certification public key in a message digitally signed using the private key corresponding to the public key included in the request, in order to:
    a. Allow the detection of errors in the certification process;
    b. Prove the possession of the private key corresponding to the certifying public key.
3. Uses the public key included in the logical request of certificate from the requesting entity to verify the signature of the requesting entity in the submitted logical request of certificate;
4. Verifies the authenticity of the submission from the RA, according to this CPS;
5. Shall verify the signature of the RA in the logical request of certificate;
6. Verifies the logical request of certificate to verify if this has errors or omissions according to this CPS;
7. Verifies the uniqueness of the DN of the requesting entity inside its infrastructure;
8. Accepts the logical request of certificate coming from the requesting entity, whose identity was validated;
9. When detecting repeated public keys the logical request of certificate shall be rejected.

### 4.2.2 In-Person Authentication of the Individual Entities

In-person authentication of the authorized representative of the candidate organizations to a certificate shall be based on at least two ways of identification issued by the government (in which, at least one has to be a document with photograph, such as a passport). The capacity of the person to act in name of the candidate organization shall also be authenticate through the presentation of documentation in paper, including this fact.

The information described above shall be validated by MULTICERT by the time of the return of the filled registration forms. MULTICERT shall be responsible for personally verify the identity of the representatives.

# 4.3 Identification and Authentication for Key Renewal Requests

## 4.3.1 Identification and authentication for routine key renewal

Many implementations of the PKI allows for the issuing, automatic or facilitated, of update certificates for a subscriber before the end of the validity period of the existing certificate. This action is known as routine renewal, and it is possible due to the fact that there is already a trust relation with the subscriber.

However, depending on the certificate in question, it is necessary to ensure that the original conditions necessary to obtain the certificate are the same, i.e.:

1. The individual/organization still exists and that he authorized the issuing of the certificate;
2. The individual/organization continues to obey to the requirements of the association;
3. The individual/organization has a private key corresponding to the new public key dispatched for certification;
4. MULTICERT accepts the continuity of the individual/organization inside its hierarchy.

The renewal may only be repeated 3 times without the need to repeat a new registration of the user. However, the Certificate Policy of the certificate to be renewed may expressly specify other renewal conditions, including contrary to this one.

## 4.3.2 Renewal after Revocation

If a certificate is revoked, the individual/organization has to do again the whole initial registration process, in order to obtain a new certificate. However, the Certificate Policy of the certificate to be renewed may expressly specify other renewal conditions, including contrary to this one.

# 4.4 Revocation Request

The revocation request shall obey to the conditions described in detail in this section 5.7.

# 5 Operational Requirements of the Certificate's Lifecycle

## 5.1 Certificate Request

The certificate request should be started with a contact to MULTICERT by telephone 217123010.

## 5.2 Issuing of the Certificates

### 5.2.1 Procedure for issuing a certificate

The issuing of the certificate is done by means of a ceremony that is held within the high security zone of MULTICERT's PKI, and where there are present:

- The legal representatives of the subordinate entity or the representative(s) named for this ceremony;
- 4 members of the Working Group since the function segregation does not allow the presence of an inferior number of elements;
- A Qualified Auditor – to testify the generation of the pair of keys from MULTICERT Root CA and issue a report relating the fulfilment of the requirements for the key generation process by MULTICERT Root CA and the use of controls to ensure the integrity and confidentiality of the key pairs;
- Any observers accepted simultaneously by the members of the Working Group and by the representatives of the requesting subordinate entity.

The ceremony of the certificate issuing is set up by the following steps:

- Identification and authentication of all the people present in the ceremony, ensuring that the representative(s) of the requesting subordinate entity and the members of the Working Group have the necessary powers for the acts to be performed;
- The representative(s) of the requesting subordinate entity hand over the CD/DVD and the issuing form of the certificate to the members of the Working Group from MULTICERT Root CA. The form is dated and signed by the members of the Working Group, who then return it to the representative(s) of the requesting subordinate entity;
- The members of the Working Group perform the procedure for the processing start from MULTICERT Root CA and issue the certificate (corresponding to the PKCS#10 supplied on the CD/DVD) in PEM format;
- The members of the Working Group archive the certificate in PEM format on a CD/DVD and fill-in in duplicate the certificate reception and acceptance form;
- After the signature of both copies of the certificate reception and acceptance form by the representative(s) of the subordinate entity and by the members of the Working Group, the members of the Working Group shall deliver the CD/DVD with the certificate in PEM format to the representative(s) of the subordinate entity;

- The issuing ceremony is concluded with the performance of the procedure for the end of the processing from MULTICERT Root CA by the members of the Working Group.

The issued certificate comes into force at the moment it is issued.

### 5.2.2 Subscriber Notification as to the Issuance of a Certificate

The issuing of the certificate is done in-person, according to the previous section.

## 5.3 Certificate Acceptance

### 5.3.1 Procedure for Accepting a Certificate

The certificate is considered accepted after the certificate reception and acceptance form by the representative(s) of the subordinate entity, according to the issuing ceremony (according to section 5.2.1).

Note that before the certificate is made available to the representatives, and consequently all functionalities for use of the private key and certificate are made available, the following should be guaranteed:

a) The rights and responsibilities are known;

b) The functionalities and content of the certificate are known;

c) The certificate and utilisation conditions are formally accepted signing for that purpose the certificate Reception Form.

### 5.3.2 Publishing of the Certificate

MULTICERT Root CA shall not publish the issued certificates, making them available integrally to the representatives, with the constraints defined in point 5.3.1.

### 5.3.3 Notification of Issuance of a Certificate to Other Entities

Nothing to remark.

### 5.3.4 Use of the Certificate and Private Key by the Subscriber

Certificate subscriber (representatives) shall use their private key only for the purpose for which these are meant (as set forth in the certificate's "*keyUsage*" field) and always for legal purposes.

Its use is only allowed:

a) By whomever is designated within the certificate's "*Subject*" field;

b) According to the conditions defined in this section 2.4;

c) While the certificate is valid and not in the CRL from MULTICERT Root CA.

Additionally:

- The certificate of the subordinate CA shall only be used to sign certificates and related CRL, as well as certificates necessary for the operation and services of the subordinate CA;
- The purpose of the certificate for the OCSP *online* validation is its use in OCSP servers;

### 5.3.5 Use of the Certificate and Public Key by Trusting Parties

In using the certificate and the public key, the trusting parties can only trust on the certificates, keeping in mind only what is established in this CPS and in the related Certificate Policy. For that, they should, among others, ensure the fulfilment of the following conditions:

a) have knowledge and understand the use and functionalities provided by the cryptography of the public key and certificates;

b) Be responsible for its correct use;

c) Read and understand the terms and conditions described in the certification Policies and practices;

d) Check the certificates (validation of chains of trust) and CRL, paying special attention to the extensions marked as critical and the purpose for the keys;

e) Trust the certificates, using them whenever they are valid.

## 5.4 Certificate Renewal

The renewal of a certificate is process in which the issuing of a new certificate uses the certificate's previous data, with no changes in the keys or any other information taking place, except for the certificate's validity period.

This practice is not sustained by MULTICERT's PKI.

### 5.4.1 Reasons for Renewing a Certificate

Nothing to remark.

### 5.4.2 Who can Submit a Certificate Renewal Request

Nothing to remark.

### 5.4.3 Processing of a Certificate Renewal Request

Nothing to remark.

### 5.4.4 Notification of the Subscriber as to the Issuance of a New Certificate

Nothing to remark.

### 5.4.5 Procedures for Certificate Acceptance

Nothing to remark.

### 5.4.6 Publication of the Certificate after Renewal

Nothing to remark.

### 5.4.7 Notification of Issuance of a Certificate to Other Entities

Nothing to remark.

## 5.5 Renewal of a Certificate with Generation of a New Key Pair

The renewal of certificate keys (*certificate re-key*) is a process in which the subscriber generates a new key pairs and submits the request for issuance of a new certificate that certifies the new public key. This process, within the scope of MULTICERT's PKI, is designated by renewal of the certificate with the generation of a new key pair.

The renewal of the certificate with the generation of a new key pair is done according to that set forth in section 5.2.

### 5.5.1 Reasons for Renewing a Certificate, Generating a New Key Pair

It is considered a valid reason for renewing a certificate, generating a new key pair, whenever:

a) The certificate is expiring;

b) The key pair is reaching the foreseen period of use;

c) The information that originated the certificate undergoes changes.

### 5.5.2 Who can Submit a Certification Request for a New Public Key

As in section 5.1.

### 5.5.3 Processing of the Certificate Renewal Request with Generation of a New Key Pair

As in section 5.2.

### 5.5.4 Notification of the Subscriber as to the Issuance of a New Certificate

As in section 5.2.2.

### 5.5.5 Procedures for Acceptance of a Renewed Certificate with Generation of a New Key Pair

As in section 5.3.1.

### 5.5.6 Publication of a Renewed Certificate with the Generation of a New Key Pair

As in section 5.3.2.

### 5.5.7 Notification of Issuance of a Renewed Certificate to Other Entities

As in section 5.3.3.

## 5.6 Changes in Certificates

Changes in certificates are a process by which a subscriber is issued a certificate, maintaining the respective keys, with only a few changes being made insofar as certificate information.

This practice is not sustained by MULTICERT's PKI.

### 5.6.1 Reasons for Changing the Certificate

Nothing to remark.

### 5.6.2 Who can Submit a Certificate Change Request

Nothing to remark.

### 5.6.3 Processing of a Certificate Change Request

Nothing to remark.

### 5.6.4 Subscriber Notification as to the Issuance of a Changed Certificate

Nothing to remark.

### 5.6.5 Procedures for Acceptance of a Changed Certificate

Nothing to remark.

### 5.6.6 Publication of the Changed Certificate

Nothing to remark.

### 5.6.7 Notification of Issuance of a Changed Certificate to Other Entities

Nothing to remark.

## 5.7 Certificate Suspension and Revocation

### 5.7.1 Circumstances for Suspension

MULTICERT Root CA does not do suspensions.

### 5.7.2 Who can Request the Suspension

Nothing to remark.

### 5.7.3 Procedure for a Suspension Request

Nothing to remark.

### 5.7.4 Limited Time Period for Suspension

Nothing to remark.

### 5.7.5 Reasons for the Revocation

A certificate can be revoked by any one of the following reasons:

1. Compromising or suspicion of compromising of the private key (from MULTICERT Root CA or Subordinate Certification Authority)
2. Loss of the private key;
3. Inaccuracies in the supplied data;
4. Loss, destruction, or deterioration of the support device for the private key (for example, cryptographic support/*token*);
5. Use the certificate for abusive activities;
6. Risk of key compromise (for example, due to the weakness of the algorithm or key size)
7. Termination of duties.

The Certificate is revoked no later than seven days.

### 5.7.6 Revocation Request

Having the legitimacy to submit a revocation request, whenever any of the conditions described in point 5.7.5 are witnessed, are the following:

1. The legal responsible for the Certification Authority;
2. MULTICERT S.A.;
3. A trusting party, whenever it is shown that the certificate was used for purposes other than those foreseen.

MULTICERT Root CA keeps all the documentation used to verify the identity and authenticity of the entity that does the revocation request, ensuring the verification of the identity if its legal representatives  verification by a legally recognized mean, not accepting representation powers for the request of certificate revocation from Subordinate Certification Authority.

### 5.7.7 Procedure for a Revocation Request

The procedures followed in the certificate revocation request are the following:

1. All the revocation requests shall be addressed to MULTICERT S.A. by writing or by digitally signed e-mail message, by appropriate form for revocation request;
2. Identification and authenticity of the entity that does the revocation request;
3. Registration and archive of the revocation request form;
4. Analysis of the revocation request by the Authentication Working Group from MULTICERT's PKI, that proposes to the Management Working Group the approval or refusal of the revocation request;
5. According to the opinion of the Authentication Working Group from MULTICERT's PKI, the Management Working Group decides upon the approval or refusal of the certificate revocation request;
6. Whenever it is decided to revoke a certificate, the revocation is published in the respective CRL.

In any case, the detailed description of the whole decision process is archived, and the following is documented:

1. Date of the revocation request;
2. Name of the certificate subscriber;
3. Detailed exposure of the reasons for the revocation request;
4. Name and functions of the person who requests the revocation;
5. Contact information of the person who requests the revocation;
6. Signature of the person who requests the revocation;

### 5.7.8 Processing the Revocation Request

The revocation request should be treated immediately, and therefore, shall not take more than 7 days, Trusting Party Verification Requirements as to Revocation.

Before using a certificate, the trusting parties have the responsibility to verify the status of all the certificates, through CRL or a verification server as to *online* status (via OCSP).

### 5.7.9 CRLs Issuing Frequency (if applicable)

MULTICERT Root CA shall publish a new CRL in its repository whenever there is a revocation. When there are no changes to the validity status of the certificates, i.e. if no revocation is produced, MULTICERT Root CA makes a new CRL available every 4 months.

The maximum time period between issuing and publishing of the CRL shall not exceed 30 minutes.

All CRLs issued by MULTICERT are digitally signed by MULTICERT or by an entity designated by MULTICERT.

MULTICERT assures that under normal operating conditions, it maintains the resources that allow a response time of 10 seconds for obtaining the CRL.

### 5.7.10 CRLs Verification Requirements

The most updates information over the revocation status of a certificate is available through servers with status verification services supplied by MULTICERT. All the interested parties should consult these server to get the most recent information over the status of a certificate.

### 5.7.11 Other Ways for Revocation Notice

MULTICERT Root CA has *online* OCSP validation services of the certificate status. That service may be accessed in http://ocsp.multicert.com/ocsp/.

## 5.8 Key Change

All Subordinate Certification Authorities recognized by MULTICERT Root CA, shall be notified (orally or by electronic means) before the update of its key pair. The notification of all the structure directly below, down to the digital certificate subscribers shall be the entire responsibility of the Subordinate Certification Authorities.

# 6 Physical Safety, Management, and Operating Measures

MULTICERT has implemented several rules and policies focusing on physical, procedural and human controls that support the security requirements present on this CPS. This section briefly describes the non-technical security aspects that allow to perform the key generation, subscriber authentication, certificate issuing, certificate revocation, audit and archive functions in a safe way. All these non-technical security aspects are critical to ensure the certificate trust, since any security shortage may compromise the operations of MULTICERT's PKI.

## 6.1 Physical Safety Measures

### 6.1.1 Physical Location and Construction Type

The facilities of MULTICERT's PKI are designed so as to provide an environment capable of controlling and auditing access to the certification systems, and are physically protected from non-authorised access, damage or interference. The architecture uses the deep defence concept, i.e. by security levels, ensuring that the access to a higher security level is only possible when we have previously reached the immediately prior level, and it is not possible for any location within the facilities to have access to safety level (n) from another level other than level (n-1).

The operations from MULTICERT's PKI are performed in a high security zone, inserted in another high security zone, and inside a building that combines several security conditions, namely the total access control that prevents, detects and hinders unauthorized accesses based on multiple physical security levels.

The two high security zones are areas that obey to the following characteristics:

a) Masonry, concrete or brick walls;

b) Ceiling and floor with similar construction to the walls;

c) Nonexistence of windows;

d) Security door, with steel plate, with fixed hinges and steel doorpost, with security lock electronically activated, fire-resistant characteristics and a panic functionality.

Additionally, the following security conditions are ensured in MULTICERT's PKI environment:

- Clearly defined security perimeters;
- Masonry walls, ceiling and floor, no windows, which hinder unauthorized accesses;
- High security anti-theft bolts and locks on the access doors to the security environment;
- The building perimeter is tightly closed since there are no doors, windows or any other uncontrolled openings that allow unauthorized accesses;
- The access to the environment necessarily passes through human-control areas and through other control means that restrict the physical access only to duly authorized personnel.

### 6.1.2 Physical Access to the Location

MULTICERT's PKI systems are protected by, at least, 4 hierarchical physical security levels (the building itself, high security block, high security area, high security room) according to NT D-02[3], ensuring that the access to a higher security level is only possible when one has previously reached the necessary privileges for the immediately prior level.

Sensitive operational activities from the CA, creation and storage of cryptographic material, any activities in the scope of the life cycle of the certification process, as authentication, verification, and issuing are performed inside the most restrict high security zone. The access to each security level requires the use of an authentication magnetic card (yellow for the building, and red for the other levels). Physical accesses are automatically registered and recorded on a TV closed circuit for audit purposes.

The access to the red identification card requires a double individual access authentication control. The entrance and stay in security areas is not allowed to unaccompanied personnel, including unauthenticated employees or visitors. Unless all personnel who move around these security areas is guaranteed recognized by all, it is required the use of the respective access card in a visible way as to ensure that no unrecognised individuals move around without the respective access card visible.

The access to the most restrict high security zone requires a double control, each using tow authentication factors, including biometric authentication. The cryptographic *hardware* and physical *tokens* have additional protection, and are kept in safe vaults and cabinets. The access to the most restrict high security zone, as well as to cryptographic *hardware* and to safe physical *tokens* is restricted, according to the responsibility segregation needs of the several Working Groups.

### 6.1.3 Energy and Air Conditioning

The security environment of MULTICERT's PKI has redundant equipment, which ensures 24 hours a day, 7 days a week operation conditions of:

- Energy feeding ensuring uninterrupted feeding systems with enough power to maintain an autonomous electrical network during periods when power is off and to protect the equipment in case of electrical surges that may damage it (the redundant equipment consists of uninterrupted power supply batteries, and diesel electric generators); and
- Refrigeration/ventilation/air conditioning, that control the temperature and humidity levels, ensuring adequate conditions for the correct operation of all the electronic and mechanical equipment present inside the environment. A temperature sensor activates a GSM alert whenever the temperature reaches abnormal values. This GSM alert consists of phone calls with a previously recorded message to the maintenance team elements.

### 6.1.4 Exposure to Water

High security zones have the proper mechanisms installed (flood detectors) to minimize the flood impact in the systems of MULTICERT's PKI.

[3] GNS/NT D-02 – Physical Security Minimum Requirements for the Certifying Entities' facilities

### 6.1.5 Fire Prevention and Protection

The safe environment of MULTICERT's PKI has all the necessary mechanisms installed to prevent and extinguish fires and other flame or fume derived incidents. These mechanisms are in compliance with the existing regulations:

- Fire detection and alarm systems are installed on the several security physical levels;
- Fixed and mobile fire extinguishing equipment's are available and positioned on strategically and easy access places in order to be quickly used at the beginning of a fire and successfully extinguishing it;
- Well defined emergency procedures in case of fire.

### 6.1.6 Safeguarding Storage Support

All sensitive information supports holding production *software* and data, audit information, archive or backup copies are kept in safe vaults and cabinets inside the high security zone, as well as in a distinct environment external to the building with physical and logical access controls appropriate to restrict the access only to authorized elements of the Working Groups. Besides the access restrictions, it also has accident protection mechanisms implemented (e.g., caused by water or fire).

When, for backup copy archive purposes, sensitive information is transported from the high security zone to the external environment, the process is performed under the supervision of at least 2 (two) Working Group elements, who are required to ensure the safe transport of the information to the destination place. The information (or the information transport *token*) shall be always under visual control of the Working Group members.

In situations implying the physical move of the data storage *hardware* (i.e., hard discs,...) outside the high security zone, for reasons other than the backup copy archive, each *hardware* element shall be verified the ensure that it does not hold any sensitive data. In these situation, the information may be eliminated using all necessary means (hard disc format, cryptographic *hardware reset*, or even the physical destruction of the storage equipment).

### 6.1.7 Elimination of Waste

Paper documents and material holding sensitive information shall be shredded before they are eliminated.

It is assured that it is not possible to recover any information from the information supports used to store or transmit sensitive information (through low level “safe” formatting or physical destruction), before they are eliminated. Cryptographic elements or logic access physical keys are either physically destroyed or follow the destruction recommendations of the respective manufacturer prior to its elimination. Other storage equipment’s (hard discs, *tapes*, ...) shall be duly cleaned in a way that it is not possible to retrieve any information (through safe formatting, or physical destruction of the equipment).

### 6.1.8 External Installations (alternative) for Backup Recovery

All backup copies are kept in a safe environment inside external facilities, being stored in safe vaults and cabinets placed in logic and physical access control zones, in order to restrict the access only to authorized personnel, also ensuring the protection against accidental damages (e.g., caused by water or fire).

## 6.2 Process Safety Measures

The activity of a Certification Authority (hereinafter referred to as CA) depends on the coordinated and complementary intervention of an extensive human resource members, namely because:

- Given the inherent security requirements to the operation of a CA, it is vital to ensure a proper responsibility segregation, which minimizes the individual importance of each participant;
- It is necessary to ensure that the CA can only be subject to *denial-of-service* type of attacks by means of collusion by a significant number of participants;
- When one entity holds several CAs from different hierarchy or security levels, it is sometimes desirable that the human resources connected to a CA do not combine functions (or at least the same) in a distinct CA.

For this reason, this section describes the necessary requirements to recognize the trust roles and the responsibilities associated with each of those roles. This section includes the duties separation, in terms of the roles that cannot be performed by the same individuals.

### 6.2.1 Working Groups

As authenticated people are defined all employees, suppliers, and consultants who have access to or control the cryptographic or authentication operations.

MULTICERT's PKI has established that the trust roles should be grouped in seven different categories (which correspond to six distinct Working Groups) in order to ensure that the sensitive operations are performed by different authenticated people, eventually belonging to different Working Groups.

#### 6.2.1.1 Audit Working Group

Is responsible for performing the internal audit to the relevant and necessary actions to ensure the CA's operability. This group shall have at least 2 (two) members.

This group's responsibilities are:

- To audit the performance and to confirm the accuracy of the CA's processes and ceremonies;
- To register all sensitive operations;
- To investigate procedural fraud suspects;
- To regularly verify the functionality of the security controls (alarm devices, access control devices, fire sensors, etc.) present in the several environments;
- To register all auditable procedures;
- To register the results of all the actions they perform;
- To assume the role of “System Auditor”[4];
- To validate that all used resources are secure.

Additionally[5]:

[4] cf. Regulatory Decree No. 25/2004, from July 15th, Article 29.

[5] cf. Regulatory Decree No. 25/2004, from July 15th, Article 30.

- The external auditor shall be independent from the certification authority, shall have recognized competence, experience, and solid qualifications in the information security area in the performance of security audits and in the use of *standard* ISO/IEC 17799; and needs to be accredited by the "National Security Authority";
- The Certification Authority needs to make proof, through an annual audit and a security report (produced by an accredited security auditor) that the risk assessment was analysed and that all necessary measures for information security were identified and implemented;
- The security auditor needs to ensure that none of its members performs partial or discriminatory roles connected to the Certification Authority. It also needs to ensure that none of its auditors ever worked for the Certification Authority in the last 3 years, nor have they any type of agreement or legal contract with the Certification Authority.

### 6.2.1.2 Operation Working Group

Is responsible for performing the routine tasks essential to the proper functioning and correct operation of the CA. This group's responsibilities are:

- Management of the "Production Environment" and of the "Operation Environment";
- To perform the CA's routine tasks, including backup copy operations of its systems,
- To perform the CA's system monitoring tasks;
- To monitor, report and quantify all *software* and *hardware* incidents and malfunctions, triggering the appropriate correction processes;
- To assume the role of "System Administrator"[4];
- To assume the role of "System Operator"[4] and;
- To assume the role of "Registration Administrator"[4];

None of the members from this group are allowed to enter on the "Production Environment" without the presence of at least one member belonging to another working group.

### 6.2.1.3 Authentication Working Group

Is responsible for proposing all the AC politics, ensuring that those politics are updated.

Is also responsible for ensuring the management, safeguard and availability (in the foreseen situations) of the (non-personal) passwords and authorization *tokens*. None of the members from this group are allowed to enter on the "Production Environment" without the presence of at least one member belonging to another working group.

This group's responsibilities are:

- Define all politics of the AC and ensure that they are updated and adapted to its reality;
- Ensure that the CP's of the AC are supported by the CPS of the AC;
- Ensure that all relevant documents, related directly or indirectly with the operation of the AC are stored in the Information Environment;
- Management of the "Authentication Environment";
- Management of all non-personal passwords;

- To keep an updated inventory of all the authentication *tokens* used in the “Operation environment”, and when the *tokens* are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the “Authentication Environment”;
- To keep an updated inventory of all the passwords used in the “Operation environment”, and when the passwords are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the “Authentication Environment”;
- To ensure that each member of the remaining groups do not hold any more authentication *tokens* than what is strictly necessary to perform the entrusted responsibilities;
- To ensure that each member of the remaining groups do not hold any more authentication passwords than what is strictly necessary to perform the entrusted responsibilities;
- To register the return of the authentication *tokens* used by the members of the remaining groups;
- To register the return of the authentication passwords used by the members of the remaining groups;
- To register the loss of authentication *tokens*, properly describing the originating situation;
- To always register when an authentication password is compromised, properly describing the originating situation;
- To assess the business risks deriving from the loss of a *token* or the compromising of an authentication password;
- To take active measures not to compromise each Production Environment deriving from the loss of a *token*, or the compromising of any authentication password, and
- To assess the documentation replication requests;
- To assume the *Security Administrator* role, as defined by Article 29 in the Portuguese Regulatory Decree No. 25/2004.

#### 6.2.1.4 Monitoring and Control Working Group

The mission of this group consists in the monitoring consolidation and analysis of the security control points of all the resources used in MULTICERT's PKI, which may lead to events, alarms and incidents.

Taking this framework into account, the Monitoring and Control Working Group interacts with the Audit Working Group to contribute to the effort for continuous improvement of the security commitments of MULTICERT's PKI, still assuming a relevant role in the incident control and related management process.

This group's responsibilities are:

- To install and configure the base *software* from MULTICERT's PKI;
- To install, interconnect, and configure the *hardware* from MULTICERT's PKI;
- To configure the initial passwords, which will be later changed by the Authentication Working Group, and
- The prepare notices about:

  - The initial passwords;
  - *Hash* of the used installation CD(s);
- The list of all the artefacts (unequivocally identified) essential for the initialization, and operation of the PKI. To consolidate and analyse the monitoring of the used resources in MULTICERT's PKI;
- To ensure the continuous improvement to the "Incident management process" and related operational management;
- To collaborate with the Audit Working Group with the purpose to promote continuous improvement actions;
- To monitor the operation of the existing alarms;
- To make production passages required by post-production;
- To monitor events, manage alarms and classify incidents;
- To define, support the implementation and continuous improvement of incident response procedures;
- To make production passages required by post-production.

#### 6.2.1.5 Management Working Group

Is responsible for naming the members for the remaining groups[6] and for the safekeeping of some sensitive artefacts (authentication *tokens*, etc.). This group shall have at least 4 (two) members.

This group's responsibilities are:

- Management of the "Management Environment";
- To review and approve the policies proposed by the Authentication Working Group;
- To name the members for the remaining Working groups (except for the Installation Working Group, the Audit Working Group, and Custody Working Group);
- To make the identification of all the individuals belonging to the different Working Groups available in one or more access points, easily accessible by authorized individuals.

#### 6.2.1.6 Custody Working Group

Is responsible for the custody of some sensitive artefacts (authentication *tokens*, etc.), which may be collected by the members of the other Working groups by the fulfilment of certain conditions[7]. Please note that, in order to improve the security levels, the business operability and continuity of the CA, there may exist several instances of this group, each in charge of the custody of a distinct set of artefacts. This group shall make use of the several safe environments available for the safekeeping of this type of items.

This group's responsibilities are:

- Management of the respective "Custody Environment";

[6] Except for the Installation Work Group, the Audit Work Group, and Custody Work Group

[7] Defined for each of the artefacts to its guard

- Custody of sensitive artefacts (authentication *tokens*, etc.) using the proper means to respond to the respective security needs, and
- Safe provision of these items to members of authorized groups and explicitly indicated having access permissions to these items, after the fulfilment of the appropriate security procedures.

### 6.2.2 Number of Persons Demanded per Task

There are rigorous control procedures that require the division of responsibilities based on the particularity of each Working Group, and in order to ensure that sensitive tasks can only be performed by a multiple group of authenticated people.

The internal control procedures were elaborated in order to ensure a minimum of 2 authenticated individuals to be able to have physical and logical access to the security equipment. The access to the CA's cryptographic *hardware* follows strict procedures involving multiple individuals authorized to access to it during its life cycle, from reception and inspection to physical and/or logical destruction of the *hardware*. After the activation of a module with operational keys, additional access controls are used in order to ensure that the physical and logical accesses to the *hardware* are only possible with 2 or more authenticated individuals. The individuals with physical access do not hold the activation keys and vice-versa.

### 6.2.3 Functions that Require Segregation of Duties

The following matrix defines the incompatibilities (marked with ✗) between belonging to the group/subgroup identified in the left column and belonging to the group/subgroup identified in the first row, under the scope of this CA:

| **May belong to the Group?**<br>**If belonging to the Group/Subgroup ...** | **Operation** | **Authentication** | **Audit** | **Custody** | **Management** |
|---|---|---|---|---|---|
| **Operation** | ▨ | ✗ | ✗ | ✗ | ✗ |
| **Authentication** | ✗ | ▨ | ✗ | ✗ | ✗ |
| **Audit** | ✗ | ✗ | ▨ | ✗ | ✗ |
| **Custody** | ✗ | ✗ | ✗ | ▨ | ✗ |
| **Management** | ✗ | ✗ | ✗ | ✗ | ▨ |

## 6.3 Personnel Safety Measures

### 6.3.1 Requirements Regarding the Qualifications, Experience, Background, and Accreditation

All personnel who perform trust functions in MULTICERT's PKI shall comply with the following requirements:

- Was formally appointed to the function to perform;
- Present proof of the background, qualifications, and experience necessary to perform the tasks inherent to his/her function;
- Has a minimum accreditation to National Confidential (or equivalent);
- Has proper training and experience to perform the respective function;
- Ensures confidentiality regarding sensitive information about de CA or subscriber identification data;
- Ensures the knowledge of the terms and conditions to perform the respective function, and
- Ensures that does not perform any function that may cause conflict with the responsibilities in the CA's activities.

### 6.3.2 Background Check Procedures

Background checks result from the accreditation process of individuals nominated to hold positions in any one of the trust functions. The background check[4] includes:

- Identification confirmation using the documentation issued by reliable sources, and
- Criminal records investigation.

### 6.3.3 Training and Experience Requirements

Adequate training and experience is given to the members of the Working Groups in order to perform their tasks in a satisfactory and competent manner.

The Working Group elements are additionally subject to a training and experience plan, including the following topics:

a) Digital certification and Public Key Infrastructure;

b) General concepts on information security;

c) Specific training for their role inside the Working Group;

d) Operation of *software* and/or *hardware* used in MULTICERT's PKI;

e) Certificate Policy and Certification Practices Statement;

f) Disaster Recovery;

g) Procedures for the activity continuity, and

h) Basic legal aspects regarding the certification services.

### 6.3.4 Frequency and Requirements for Recycling Actions

Whenever necessary, complementary training and experience shall be provided to the Working Group members, in order to ensure the required professional level for the competent and satisfactory performance of their responsibilities. In particular,

- Whenever there are any technological change, introduction of new tools or changes in the procedures, an adequate training is given to all personnel allocated to MULTICERT's PKI;
- Whenever there are changes introduced to the Certificate Policies or Certification Practices Statement recycling sessions are held for all the elements of MULTICERT's PKI.

### 6.3.5 Frequency and Sequence of Function Rotation

Nothing to remark.

### 6.3.6 Sanctions for Unauthorised Actions

Unauthorized actions are considered to be all actions that disrespect the Certification Practices Statement and the Certificate Policies, whether deliberately or by negligence.

Sanctions are applied according to the rules from MULTICERT's PKI and the national security laws to all the individuals who perform unauthorized actions or make unauthorized use of the systems.

### 6.3.7 Requirements for Service Providers

Independent consultants or service providers have permission to access the high security zone as long as they are escorted and directly supervised by the Working Group members, and their access is registered in the appropriate Presence Book.

### 6.3.8 Documentation Provided to Personnel

All adequate information is made available to the Working Group members so they can perform their tasks in a competent and satisfactory manner.

## 6.4 Security Audit Procedures

### 6.4.1 Type of Registered Events

Significant events that generate auditable records. These include at least the following:

- Access attempts (with or without success) to request, generate, sign issue or revoke certificate keys;
- Access attempts (with or without success) to create, modify or erase subscriber certificate information;
- Access attempts (with or without success) to change the security parameters of the operating system;

- CRLs issuing and publication;
- Application start and stop;
- Access attempts (with or without success) to initiate and terminate sessions;
- Access attempts (with or without success) to create, modify, or erase system accounts;
- Backup copies, data recovery or storage;
- *Software* and *hardware* changes or updates;
- System maintenance;
- Operations performed by Working Group members;
- Human resource change;
- Access attempts (with or without success) to the facilities by authorized or not personnel;
- The ceremony for the key generation and systems involved, such as application servers, databases and operating system.

The entries in the records include the following information:

- Serial number of the event;
- Date and time of the event;
- Identity of the individual who caused the event;
- Category of the event, when applicable;
- Description of the event.

### 6.4.2 Frequency of the Records Audit

The records are analysed and reviewed by the Audit Working Group elements, and additionally every time there are suspicions or abnormal activities or threats of any kind. The actions taken, based on the records information are also documented.

### 6.4.3 Retaining Period for Auditing Records

The records are maintained for at least 2 (two) months after processing, and then stored under the terms described in this section 6.5.

### 6.4.4 Protection of the Auditing Records

The records are exclusively analysed by the Audit Working Group members and reported to the Management Group.

The records are protected by auditable electronic mechanisms in order to detect and hinder the attempt of unauthorized data changes, removal or any other manipulation schemes.

Backup copies from MULTICERT's PKI are stored in a safe place and in vaults in compliance with standard EN 1143.

The destruction of an audit archive can only be made after the express authorization of the Management Group and performed in the presence of at least two elements, one from authentication and one from audit, and it shall be registered in an Audit log.

### 6.4.5 Record Backup Copy Procedures

Backup copies are regularly created in high capacity storage systems, in *tape* and in *storage*.

### 6.4.6 Record Collection System (Internal / External)

The audit record treatment and collection process is constituted by a combination of automatic and manual processes executed by the operating systems, by MULTICERT's PKI applications, and by the personnel operating it. All audit records are stored in MULTICERT's PKI internal systems.

### 6.4.7 Notification of the Agents Causing the Events

Auditable events are registered in the audit system and stored in a safe way, without notification to the event causing subject.

### 6.4.8 Assessment of Vulnerabilities

The auditable records are regularly assessed in order to minimize and eliminate potential attempts to break the system security.

Two intrusion tests are performed each year in order to check and assess the vulnerabilities.

The analysis result is reported to MULTICERT's PKI Management Group to review and approve an implementation and correction plan for the detected vulnerabilities.

## 6.5 Record Storage

### 6.5.1 Type of Data Stored

All auditable data are stored (as indicated in section 6.4.1), as well as information about the certificate requests and support documentation to the life cycle of the different operations.

The information and events that are recorded and stored are:

a) Audit records specified in point 6.4.1 of this CPS;

b) The system backup copies that make up MULTICERT's PKI infrastructure;

c) All documentation related to the life cycle of the certificates, namely:

- Service certificate issuing and revocation procedures;
- Service certificate issuing and reception forms;

d) Confidentiality agreements;

e) Protocols established with the Subscribing Entities;

f) Contracts established between MULTICERT' PKI and other entities - made available only to those asking to view it after previous assessment and approval of the request;

g) Access authorizations to the information systems;

h) Accesses to the existing artefacts in custodies.

### 6.5.2 Period for Retaining Stored Files

The data subject to storage are retained by the period of time defined by national legislation.

### 6.5.3 Archive Protection

The archive is protected in order to:

- Only authorized members of the Working Group may consult and access to the archive;
- The archive is protected against any change or attempt to remove it;
- The archive is protected against the deterioration of the media where it is stored, through the regular migration to a new media;
- The archive is protected against obsolescence of the *hardware*, operating systems and other *software*, through the conservation of the *hardware*, operating systems and other *software* which then make part of the archive itself, in order to allow the access and use of the stored records in a timeless manner;
- The archives are stored in a safe manner in safe external environments. Backup copies from MULTICERT's PKI are stored in safe places and in vaults in compliance with standard EN 1143.

### 6.5.4 Procedures for the Backup Copies of the Archive

Backup copies of the archives are done in an incremental or total manner and stored in WORM (*Write Once Read Many*) devices.

### 6.5.5 Requisites for Chronological Validation of the Records

Some entries in the archives may contain date and time information. That date and time information is not based on a safe time source.

### 6.5.6 Stored Data Collection System (Internal/External)

The stored data collection systems are internal.

### 6.5.7 Procedures for Recovering and Checking Stored Information

Only authorized members of the Working Groups have access to the archives to check its integrity.

Integrity automatic checks are performed to the electronic archives (backup copies) at the time of its creation, in case of errors or unpredicted behaviours a new archive should be created.

## 6.6 Key Renewal

Only Certification Authorities subordinated to MULTICERT's PKI with valid certificates may require the renewal of the respective key pair, as long as the creation of the new key pair is compliant with section 6.7.

## 6.7 Recovery in Case of Disaster or Compromise

This section describes the requirements related to the notification and recovery procedures in case of disaster or compromise.

### 6.7.1 Procedures in Case of Incidents or Compromise

The backup copies of private keys from MULTICERT Root CA (created and stored according to section 7.2.3.1) and of the archived records (section 6.5.1) are stored in external safe environments and available in case of disaster. In case of compromise of the private key from MULTICERT Root CA, this shall perform the following actions:

- To proceed to its immediate revocation;
- To revoke all its dependent certificates;
- To inform all its certificate subscribers and known third parties;
- To inform all Entities that constitute MULTICERT's PKI.

### 6.7.2 Corruption of the Computer Resources, *Software* and/or Data

In case the computer resources, *software* and/or data are compromised or corruption is suspected, the backup copies of the private keys from the CA and the archived records may be obtained to check the integrity of the original data.

If it is confirmed that computer resources, *software* and/or data are corrupted, appropriate measures shall be taken to respond to the incident. The response to the incident shall include the recovery of the corrupted equipment/data, using similar equipment and/or recovering stored backup copies and records. Until the safe conditions are restored, MULTICERT CA Root shall suspend its services and notify all involved Entities. In case this situation has affected issued certificates, its subscribers shall be notified and the respective certificates shall be revoked.

### 6.7.3 Procedures in Case the Entity's Private Key is Compromised

In case the private key from MULTICERT Root CA is compromised or there is a suspicion of its compromise, appropriate measures shall be taken to respond to the incident. The responses to that incident may include:

- Inform the National Security Authority (ANS);
- Revocation of the certificate from MULTICERT Root CA and all certificates issued in the trust hierarchy "branch" from MULTICERT Root CA;
- Notification of the subordinate CA, and all the subscribers of certificates issued in the trust hierarchy "branch" from MULTICERT Root CA;

- Creation of a new key pair for MULTICERT Root CA and inclusion in the different systems/*browsers*;
- Revocation of all certificates issued in the trust hierarchy "branch" from MULTICERT Root CA;

### 6.7.4 Capacity to Continue the Activity in Case of Disaster

MULTICERT's PKI has the computing resources, *software*, backup copies and records stored in its safe secondary facilities, necessary to restore or recover essential operations (certificate issuing and revocation with the publication of the revocation information) based on procedures defined in the Contingency Plan after a natural disaster or other.

## 6.8 Procedures in Case of Extinction of the CA or RA

In case the activity as Certification service provider ceases, MULTICERT Root CA shall with a minimum prior notice of three months proceed to the following:

a) Inform the National Security Authority (ANS);

b) Inform all involved Entities;

c) Inform all certificate subscribers;

d) Revoke all issued certificates;

e) Provide a final notification for subscribers 2 (two) days prior to formal cessation of the activity;

f) Destroy or prevent the use, in a definite manner, of the private keys;

g) Guarantee the transfer and maintenance (to be retained by another organisation) of all information relative to the CA's activity, namely CA key, certificates, documentation stored (internally or externally), repositories and event records storage during the period of time legally required .

In case of changes in the responsible CA activity managing body/structure, it shall inform the entities listed in the previous lines of that fact.

# 7 TECHNICAL SAFETY MEASURES

This section defines the security measures implemented by MULTICERT's PKI for MULTICERT Root CA, in order to protect the cryptographic keys it issued and related activation data. The security level assigned to the key maintenance shall be the highest in order for private keys and safe keys, as well as activation data, to be always protected and only accessed by duly authorized people.

## 7.1 Generation and Installation of the Key Pair

The generation of key pairs from MULTICERT Root CA is processed in accordance with the requirements and algorithms defined in this policy.

### 7.1.1 Generation of the Key Pair

The creation of cryptographic keys from MULTICERT Root CA is done by a Working Group, composed by authorized elements for that purpose, in a ceremony planned and audited according to the written procedures for the operations to perform. All key creation ceremonies are registered, dated and signed by the elements involved in the Working Group.

The cryptographic *hardware* used for the creation of keys from MULTICERT Root CA, is compliant with the FIPS 140-2 level 3 and/or *Common Criteria* EAL 4+ requirements, and performs the key maintenance, storage, and all the operations involving cryptographic keys using the *hardware* exclusively. The access to critical keys is protected by security papers, role division between the Working Groups, as well as through user limited access rules. The backup copies from cryptographic keys are done using only the *hardware*, thus allowing the proper audit of these copies, and a full and safe recovery of the keys may be possible in the event of a data loss.

The creation of the key pair from MULTICERT Root CA is done by authorized elements from the Working Groups on a cryptographic *hardware* compliant with FIPS 140-2 level 3 and/or *Common Criteria* EAL 4+ requirements.

The operation of MULTICERT Root CA is performed in *offline* mode.

### 7.1.2 Delivery of the Private Key to the Subscriber

MULTICERT Root CA does not creates the private key associated to the certificates that it issues.

### 7.1.3 Delivery of the Public Key to the Certificate Issuer

The public key is delivered to MULTICERT Root CA, according to the procedures mentioned in section 5.2.2.

### 7.1.4 Delivery of the CA's Public Key to the Trusting Parties

The public key from MULTICERT Root CA shall be made available through the certificate from MULTICERT Root CA, according to section 5.3.2.

### 7.1.5 Key Size

The length of the key pairs shall be enough to prevent possible cryptanalysis attacks discovering the private key corresponding to the key pair during the use period. The key size is the following:

- 4096 bits RSA for the key from MULTICERT Root CA.

### 7.1.6 Generation of the Public Key Parameters and Quality Check

The generation of the public key parameters and quality check shall always be based on the standard that defines the algorithm.

The creation of CA's keys is based on the use of random/pseudo random processes described on ANSI X9.17 (Annex C), according to the stipulated in PKCS#1.

### 7.1.7 Key Purposes (field "*key usage*" X.509 v3)

The field "*keyUsage*" on the certificates, used according to the recommendations on *RFC 5280*[8], includes the following uses:

*a) Key Certificate Signature*

*b) CRL Signature*

## 7.2 Protection of the Private Key and Features of the Cryptographic Module

In this section are considered the requirements for private key protection and for cryptographic modules from MULTICERT Root CA. MULTICERT's PKI has implemented a combination of physical and logical controls, and procedures dully documented in order to ensure private key confidentiality and integrity from MULTICERT Root CA.

### 7.2.1 Safety Standards and Measures of the Cryptographic Module

For the creation of the key pairs from MULTICERT Root CA, as well as for the storage of the private keys, MULTICERT's PKI uses a cryptographic module in *hardware*, which complies with the following standards:

- Physical Security
    - *Common Criteria* EAL 4+ and/or
    - FIPS 140-2, level 3
- Regulatory Certifications
    - U/L 1950 & CSA C22.2 *safety compliant*
    - FCC Part 15 – Class B
    - ISO – 9002 Certification
- Papers

[8] cf. RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile*

  - Two factor authentication
- Creation of random numbers
  - *ANSI* X9.17 (Annex C)

## 7.2.2 Multi-personnel Control (*n* of *m*) for the Private Key

The multi-personnel control is only used for CA keys, since the certificate's private key is under the exclusive control of its subscriber.

MULTICERT's PKI has implemented a set of mechanisms and techniques that require the participation of several members of the Working Group to perform sensitive cryptographic operations in CA.

The activation data necessary for using the private key from MULTICERT Root CA are divided in several parts (stored in the PED keys – small digital identification *tokens*, with physical key format, identifying different access roles to HSM), being accessible, and at the responsibility of the different members of the Working Group. A defined number of these parts (*n*) from the total number of parts (*m*) is necessary to activate the private key from MULTICERT Root CA stored in the *hardware* cryptographic module. Two parts (n) are necessary for the activation of the private key form MULTICERT Root CA.

## 7.2.3 Retention of the Private Key (*key escrow*)

MULTICERT Root CA only retains its private key.

### 7.2.3.1 Policies and Practices for Recovering Keys

The private key from MULTICERT Root CA is stored in a security *hardware token* and a backup copy is made using a direct connection hardware to *hardware* between two security *tokens*. The backup copy creation is the last step for issuing a new key pair from MULTICERT Root CA.

The backup copy ceremony uses a HSM with two factor authentication (portable authentication console and PED keys – small digital identification *tokens* with a USB pen format – identifying different roles in the access to HSM), where several people, each holding a PED key, are required to authenticate themselves before it is possible to make the backup copy.

The security *hardware token* with the backup copy of the private key from MULTICERT Root CA is placed in a safe vault in secondary safe facilities, and accessible only to the authorized members of the Working Groups. The physical access control to those facilities prevents that other people have unauthorized access to the private keys.

The backup copy of the private key from MULTICERT Root CA may be recovered in case of malfunction of the original private key. The key recovery ceremony uses the same two factor authentication mechanisms, and with several people, used in the backup copy ceremony.

### 7.2.3.2 Policies and Practices for Encapsulation and Recovery of the Session Keys

Nothing to remark.

## 7.2.4 Backup Copy of the Private Key

The private key from MULTICERT Root CA has at least one backup copy with the same security level as the original key.

All the key subject to backup copies are stored for at least 30 years after their expiry date.

## 7.2.5 Storage of the Private Key

The private keys from MULTICERT Root CA, subject to backup copies, are stored as identified in section 7.2.3.

## 7.2.6 Transfer of Private Keys to/from the Cryptographic Module

The private keys from MULTICERT Root CA are not extractable from the cryptographic *token* FIPS 140-2 level 3.

If a backup copy of the private keys from MULTICERT Root CA is made to another cryptographic *token*, that copy é done directly, *hardware* to *hardware*, thus ensuring the transport of the key between modules in an enciphered transmission.

## 7.2.7 Storage of the Private Key in the Cryptographic Module

The private keys from MULTICERT Root CA are stored in an enciphered way in the cryptographic *hardware* modules.

## 7.2.8 Process for Activating the Private Key

MULTICERT Root CA is an *offline* CA, whose private key is activated when the CA's system is connected. This activation is put into effect through the cryptographic module authentication by the individuals indicated for that purpose, being compulsory the use of the two factor authentication (portable authentication console and PED keys – small digital identification *tokens* with a physical key format – identifying different roles in the access to HSM), where several people (members of the Working groups), each holding a PED key, are required to authenticate themselves before it is possible to make the backup copy.

For activating the private keys from MULTICERT Root CA it is necessary at least the intervention of four elements of the Working Group. Once the key is activated, it will remain that way until the deactivation process takes place.

## 7.2.9 Process for Deactivating the Private Key

The private key from MULTICERT Root CA is deactivated when the CA's system is disconnected.

Once deactivated, it will remain inactive until the activation process takes place.

### 7.2.10 Process for Destructing the Private Key

The private keys from MULTICERT Root CA (including backup copies) are erased/destroyed in a procedure duly identified and audited, at least 30 days after the end of its expire date (or if they are revoked before that period).

MULTICERT's PKI destroys the private keys ensuring that no residue will remain that might allow its reconstruction. For that, it uses the format function (zero initialization) made available by the cryptographic *hardware* and other appropriate means, in order to ensure the destruction of the CA's private keys.

### 7.2.11 Assessment/level of the Cryptographic Module

Described in section 7.2.1.

## 7.3 Other Aspects for Managing Key Pairs

### 7.3.1 Storage of the Public Key

A backup copy of the public keys from MULTICERT Root CA is made by the members of the Working Group, and remain stored after the expiry date of the corresponding certificates, to verify the signatures generated during its validity.

### 7.3.2 Validity Periods of the Certificate and Keys

The period to use the keys is determined by the certificate's validity period, so that after the certificate expires, its keys can no longer be used, originating the permanent termination of the operability and use for which they were meant.

In this sense, the validity of the various types of certificates and the period in which these should be renewed is the following:

- The certificate from MULTICERT Root CA has a 25-year validity, being used to sign certificates during its first 12 years, and is reissued before it reaches a validity of 12 years and 6 months;
- The certificate from the subordinate CE from MULTICERT has a 12-year validity, being used to sign certificates during the first 6 years, and is reissued after it reaches a validity of; The OCSP (Online Certificate Status Protocol) certificates have a validity of 5 years and 4 months, being used during the first four months and reissued after the fourth month of validity;

## 7.4 Activation Data

### 7.4.1 Generation and Installation of Activation Data

The activation data necessary for using the private key from MULTICERT Root CA are divided in several parts (stored in PED keys – small digital identification *tokens*, with physical key format, identifying different access roles to HSM), and are at the responsibility of the different members of the Working Group. The different parts are generated according to what was defined in the process/ceremony for the key generation, and obey to the requirements defined by standard FIPS 140-2 level 3.

### 7.4.2 Protection of Activation Data

The activation data (in separate parts and/or password) are memorized and/or stored in *tokens*, that show violation attempts and/or are stored in envelops and in safe vaults.

The private keys from MULTICERT Root CA are stored in an enciphered way in cryptographic *token*.

### 7.4.3 Other Aspects from Activation Data

If there is a need to transmit the activation data from the private keys, this transmission will be protected against information loss, theft, data change and unauthorized release.

Activation data are destroyed (by format and/or physical destruction) when the associated private key is destroyed.

## 7.5 Computer Safety Measures

### 7.5.1 Specific Technical Requirements

The access to the servers from MULTICERT Root CA is restrict to the members of the Working Group with a valid reason for that access. MULTICERT Root CA works *offline*, being disconnected at the end of each certificate issuing or of any other necessary technical intervention, complying the necessary requirements for identification authentication, access control, administration, audit, reuse, service responsibility and recovery, and information exchange.

### 7.5.2 Security Assessment/level

The various systems and products used by MULTICERT Root CA, within the realm of SECS, are reliable and protected against changes.

The cryptographic module in *Hardware* from MULTICERT Root CA complies the standard EAL 4+ *Common Criteria for Information Technology Security Evaluation* and/or FIPS 140-2 level 3.

## 7.6 Lifecycle of Technical Safety Measures

### 7.6.1 System Development Measures

The applications are developed and implemented by third parties according with its rules for system development and change management.

Auditable methodology is supplied allowing to verify that the *software* from MULTICERT Root CA was not changed before it was first used. All configurations and changes of the *software* are done and audited by members of the Working Group from MULTICERT's PKI.

### 7.6.2 Safety Management Measures

MULTICERT' PKI has mechanisms and/or Working Groups to control and monitor the configuration of the CA's systems. The system from MULTICERT Root CA, when used by the first time, will be verified to ensure that the *software* used is reliable and was not changed after its installation.

### 7.6.3 Lifecycle of Safety Measures

The update and maintenance of operations of the products and systems from MULTICERT Root CA follow the same control of the original equipment and is installed by the members of the Working Group with appropriate training for the purpose, in accordance with the procedures defined.

## 7.7 Network Safety Measures

MULTICERT Root CA is an *offline* CE and is not connected to any network.

## 7.8 Chronological validation (*Time-stamping*)

Certificates, CRL's and other entries in the data base always have information about the date and hour of that entry. The chronological information is not based on a dedicated time source. The maximum offset is 60 seconds. All operations done in MULTICERT Root CA, and with this CA being *offline*, are initiated with the verification of the system date/hour.

# 8 Certificate Policy and CRL

## 8.1 Certificate Profile

The users of a public key have to trust that the associated private key is held by the correct remote subscriber (person or system) with which they will use the encipher mechanism or digital signature. The trust is obtained through the use of X.509 v3 digital certificates, which are data structure that make the connection between the public key and its subscriber. This connection is stated through the digital signature of each certificate by a trusted CA. The CA may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the subscriber.

A certificate has a limited validity period, indicated in its content and signed by the CA. Since the signature of the certificate and its validity may be independently verified by any certificate using *software*, the certificates may be distributed through communication lines and public systems, and may be stored in any type of storage units.

The user of a security system that requires the knowledge of the public key by the user, usually has to obtain and validate the certificate holding that key. If the service does not hold a trustful copy of the public key from the CA that signed the certificate, as well as the name of the CA and related information (and the validity period), then there may be required an additional certificate to obtain a public key from the CA and validate the user's public key. Generally, to validate the public key from a user, there may be needed a network of multiple certificates, including the public key certificate of the user signed by a CA, and zero or more additional certificates from CAs signed by other CAs.

The profile issued by MULTICERT Root CA is compliant with the:

- ITU.T recommendation X.509[9];
- RFC 5280[8];
- ETSI 102 042, v2.4.1;
- ETSI 101 456, v.1.4.3;
- Applicable legislation, national and European.

## 8.2 Profile of the Certificate Revocation List

When a certificate is issued, it is expected that it will be used during all its validity period. However, several circumstances may cause the certificate to become invalid before its expiry date. Such circumstances include the change of the name, of the association between subscriber and the certificate data (for example, a worker terminating his job), and the compromise or suspicion of compromise of the corresponding private key. Under such circumstances, the CA has to revoke the certificate.

The X.509 protocol defines a revocation method that involves the periodic issuing by the CA of a signed data structure called Certificate Revocation List (CRL). The CRL is a list with the time identification of the revoked certificates, signed by the CA, and made freely available on a public repository. Each revoked certificate is identified in the CRL by its serial number. When an application uses a certificate (for example, to verify the digital signature of a remote user), the application verifies the signature and

[9] cf. ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

validity of the certificate, obtains the most recent CRL, and verifies if the certificate serial number is not part of the same. Please note that a CA issues a new CRL on a regular periodic basis.

The CRL profile is compliant with the:

- ITU.T recommendation X.509[9];
- RFC 52808; and
- Applicable legislation, national and European.

The CRL profiles may be consulted in the documents of the Certificate Policies associated to this CPS, regarding to MULTICERT Root CA (section 3.2).

# 9 Compliance Audit and Other Assessments

A regular compliance inspection to this CPS and to other rules, procedures, ceremonies, and processes shall be performed by the members of the Audit Working Group of MULTICERT's PKI.

Besides the compliance audits, MULTICERT shall perform other inspections and investigations to ensure the compliance from the Certification Authority from MULTICERT's PKI with the national legislation as well as any applicable international standards. The execution of these internal audits, inspections and investigations may be delegated to an external audit entity.

In the case of certificate authorities belonging to MULTICERT's PKI but operated by other entities, MULTICERT may, whenever it sees fit, conduct internal audits to them. These entities are also required to annually deliver to MULTICERT the annual audit report, or a statement of compliance, conducted by an independent and recognized for that purpose.

MULTICERT Root CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

## 9.1 Compliance Audit and Other Assessments

MULTICERT Root CA was audited successfully and currently complies with the requirements from standard ETSI TS 102 042 and ETSI 101 456.

This audit was performed by auditors qualified for performing audits related to this standard, with experience analysing the PKI's technology, tools and related information security techniques.

## 9.2 Frequency or Reason for the Audit

MULTICERT's certification practices are subject to periodical audits, which will have the minimum periodicity stipulated by law, i.e. an annual periodicity with the issue of a report dating from March 31st from the calendar year in question. This audit shall be performed by a registered external entity and recognized for that purpose. This audit shall be performed based on the existing standards for that purpose, and its results are communicated to the accreditation entity, that may publish the result of the entire process.

In order to comply with these obligations, MULTICERT keeps a report of all the certificate life cycle operations and of all the communications held with the recognized registration/certifying. In the same way, MULTICERT obliges these entities to keep a record from the subscription requests received and processed, in which it had been involved. This record shall be stored in a data repository created for that purpose and should be able to be confirmed through the analysis of the communication records (in electronic medium or other) with the Certification Authority.

To verify the compliance of these dispositions, MULTICERT shall perform periodic audits to the registration/Certification Authorities as a way to determine the adequacy of the operational procedures and technological security levels to the supported Certificate Policies. The non-compliance of the contractual conditions may lead to the suspension and/or revocation of the issued certificate(s).

# 10 Policy Management

## 10.1 Procedure for the Specification Changes

### 10.1.1 Procedure for the CPS Change

#### 10.1.1.1 Changes List

Any change performed to the CPS from MULTICERT Root CA shall be subject to a change proposal document.

#### 10.1.1.2 Notification Mechanism

The proposed changes to policies shall be placed on the Internet and communicates do the Registration Entities.

#### 10.1.1.3 Comments

The different users of the services provided by MULTICERT Root CA (subscribers, registration, validation, *timestamping* or even Certification Authorities with which mutual trust relations have been established) may be able to comment or deliver opinions to MULTICERT or to the Registration Entities.

#### 10.1.1.4 Comment treating mechanisms

Once the comments are compiled, a formal change proposal shall be presented to the MULTICERT's PKI Management Group, together with the collected comments. The Management Group shall have the obligation to request the opinion of the Accreditation Authority over the impact of these changes on the accreditation from MULTICERT Root CA.

Once having all this information, the Management Group and the Authentication Working Group shall deliberate over the provision of the CPS's change proposals, and all the parties interested in the deliberations taken shall be notified. Subscribers shall then have a maximum 30-day period to request the termination of the contract with MULTICERT Root CA, without which the new disposals shall be taken as accepted.

#### 10.1.1.5 Period for the Changes to Come into Force

After the conclusion of this process, the changes will come into force after 30 days. Control mechanisms shall be adopted to ensure that all changes to the CPs and to the CPS are traced and an adequate mechanism for the version control is adopted.

# 10.2 Publication and Notification Policies

## 10.2.1 Publication and Notification Request

All items mentioned on the CPs and on the CPS from MULTICERT Root CA are subject to publication and notification.

Every publication and notification shall be made through MULTICERT's *site* (https://pki.multicert.com/index.html), unless the notification has a great impact on MULTICERT and on its clients.

MULTICERT Root CA may digitally sign each publication and each notification before they are placed on the respective *site*.

MULTICERT shall make available, publish or notify its clients over the:

- Adequate ways for protecting private keys;
- Associated risks to the use of any certificate issued by MULTICERT Root CA, whose technology has been discontinued.

## 10.2.2 Publication of the Updated CPS

The duly updated CPS document shall be permanently available through the URL https://pki.multicert.com/index.html.

## 10.2.3 Procedure for Approving the CPS

The validation of this CPS (and/or related CPs) and following corrections (or updates) shall be carried out by the Authentication Working Group. Corrections (or updates) shall be published as new versions of this CPS (and/or related CPs), replacing any CPS (and/or related CPs) previously defined. The Authentication Working Group shall also determine when the changes in the CPS (and/or related CPs) lead to a change in the object identifiers (OID) of the CPS (and/or related CPs).

After the validation phase, the CPS (and/or related CPs) is submitted to the Management Group, which is the entity responsible for the approval ant authorization of the changes made on this type of documents.

# 11 OTHER SITUATIONS AND LEGAL MATTERS

This section deals with business aspects and legal matters.

## 11.1 Fees

### 11.1.1 Certificate Issuance or Renewal Fees

To be identified in a formal proposal to be made by MULTICERT.

### 11.1.2 Certificate Access Fees

Nothing to remark.

### 11.1.3 Fees for Access to Information on the Status of the Certificate or Revocation

Access to information on the certificate status or revocation (CRL) is free and no fees can be applied.

### 11.1.4 Fees for other Services

The fees for the chronological validation and *online* OCSP validation services are identified in a formal proposal to be made by MULTICERT.

### 11.1.5 Reimbursement Policy

Nothing to remark.

## 11.2 Financial Responsibility

### 11.2.1 Insurance Coverage

MULTICERT has the compulsory civil liability insurance, according to article 16 of the Decree-Law no. 62/2003, from April 3rd.

### 11.2.2 Other Resources

Nothing to remark.

### 11.2.3 Insurance or Guarantee of Coverage for Users

MULTICERT has the compulsory civil liability insurance, according to article 16 of the Decree-Law no. 62/2003, from April 3rd.

## 11.3 Confidentiality of the Information Processed

### 11.3.1 Scope of Information Confidentiality

Expressly declared as confidential information is that which cannot be released to third parties:

a) The private keys from MULTICERT Root CA:

b) All information relative to auditing safety, control, and procedures parameters;

c) All information of a personal nature provided to MULTICERT's PKI during the registration process of the subscribers of certificates, unless if there is explicit authorization for its release and/or if this is not included in the content of the issued certificate;

d) Business continuity and recovery plans;

e) Transaction records, including complete records and auditing records of the transactions;

f) Information of all the documents related with MULTICERT's PKI (rules, policies, ceremonies, forms and processes), including organizational concepts, secret, confidential and/or privileged financial/commercial information, being the property of MULTICERT. These documents are entrusted to the human resources of MULTICERT's PKI Working Groups on the condition of not being used or released beyond the scope of its duties under the established terms, without the previous and explicit authorization from MULTICERT;

g) All passwords, PINs and other security elements related to MULTICERT Root CA;

h) The identification of the members of MULTICERT's PKI Working Groups;

i) The location of MULTICERT's PKI environments and its content.

### 11.3.2 Information Outside the Scope of Information Confidentiality

It is considered as information for public access:

a) Certificates Policy;

b) Certification Practices Statement;

c) CRL, and

d) All information classified as “public” (the information not expressly considered as “public” shall be considered as confidential).

MULTICERT allows the access to non-confidential information without prejudice of the security controls necessary to protect the authenticity and integrity of the information.

### 11.3.3 Responsibility for Protecting Confidential Information

The elements of the Working Groups or other entities receiving confidential information are responsible for ensuring that this is not copied, reproduced, stored, translated or transmitted to third parties by any means without the previous written consent from MULTICERT.

## 11.4 Privacy of Personal Data

### 11.4.1 Measures to Guarantee Privacy

The System for Managing the Certificate Life Cycle (SGCVC) is responsible for implementing the measures ensuring the privacy of personal data, according to the Portuguese legislation.

### 11.4.2 Private Information

It is considered private information all the information supplied to the certificate subscriber that is not available in the subscriber's digital certificate.

### 11.4.3 Information not Protected by Privacy

It is considered information not protected by privacy all the information supplied to the certificate subscriber that is available in the subscriber's digital certificate.

### 11.4.4 Responsibility to Protect Private Information

In accordance with the Portuguese legislation.

### 11.4.5 Notification and Consent for the use of Private Information

In accordance with the Portuguese legislation.

### 11.4.6 Release of Information resulting from Legal or Administrative Proceedings

Nothing to remark.

### 11.4.7 Other Circumstances for Revealing Information

Nothing to remark.

## 11.5 Intellectual Property Rights

All intellectual property rights, including those which refer to certificates, CRL, Delta-CRL issued, OID, CPS and CP, as well as any other document, property of MULTICERT's PKI belonging to MULTICERT, S.A..

The private keys and the public keys are propriety of the subscriber, independent of the physical means employed for storing them.

The Subscriber always has the right to brands, products or commercial names contained in the certificate.

## 11.6 Representations and Guarantees

### 11.6.1 Representation and Guarantees of Certification Authorities

MULTICERT's PKI is obliged to:

a) Carry out its operations in accordance with this Policy;

b) Clearly state all its Certification Practices in the appropriate document;

c) Protect its private keys;

d) Issue certificates in accordance with the X.509 *standard*;

e) Issue certificates that are compliant with the information known at the time it is issued and free from data input errors;

f) Ensure confidentiality in the data generating process for creating the signature and forwarding it through a safe procedure to the subscriber;

g) Use reliable systems and products that are protected against all changes and which ensures the technical and cryptographic safety of the certification processes;

h) Use reliable systems to store recognized certificates, that enable proving their authenticity and prevent unauthorised people from changing data;

i) Store the certificates issued without any changes;

j) Ensure that they can determine the precise date and hour in which it issued, extinguished or suspended a certificate ;

k) Employ personnel with the necessary qualifications, knowledge, and experience to provide certification services;

l) Revoke the certificates under the terms of section 5.7 of this document and publish the revoked certificates on the CRL in the repository from MULTICERT Root CA, with the frequency stipulated in section 5.7.9;

m) Publish their CPS and applicable Certificate Policies in its repository guaranteeing the access to current versions, as well as to previous versions;

n) Notify with the necessary speed, by e-mail the certificate subscribers in case the CA revokes or suspends the certificates, indicating the corresponding motive for such action;

o) Collaborate with the audits performed by the Accreditation Authority to validate the renewal of its own keys;

p) Operate in accordance with the applicable legislation;

q) Protect eventual existing keys that are under its custody;

r) Guarantee the availability of the CRL in accordance with the dispositions in section 5.7.9;

s) In case its activity ceases this shall be communicated with a minimum prior notice of two months to all subscribers of the certificates issued, as well as to the Accreditation Authority;

t) Comply with the specifications contained in the standard on Protection of Personal Data;

u) Maintain all information and documentation relative to a recognised certificate and the Certification Practices Statements in force at each moment and for fifteen years from issuance; and

v) Make the certificates from MULTICERT Root CA available.

### 11.6.2 Representation and guarantees of the Registration Entities

Nothing to remark.

### 11.6.3 Representations and Guarantees of the Subscribers

It is the obligation of the subscribers of the issued certificates to:

a) Limit and adjust the use of the certificates in accordance with the uses foreseen in the Certificate Policies;

b) Take all care and measures necessary to guarantee possession of its private key;

c) Immediately request that a certificate be revoked in the case of having knowledge or suspicion that the private key corresponding to the public key contained in the certificate has been compromised, according to section 5.7.5;

d) Not use a digital certificate that has lost its effectiveness, both due to revocation, suspension or expiration of its validity period;

e) Submit to the Certification Authority (or Registration Entity) the information that they consider accurate and complete with relation to the data that these require to carry out the registration process. The CA should be informed on any changes in this information; and

f) Not monitor, manipulate or carry out reversed engineering on the technique implemented (hardware and software) for certification services, without the previous duly authorization, in writing, from the MULTICERT's PKI.

### 11.6.4 Representation and Guarantees of the Trusting Parties

It is the obligation of the parties that are entrusted with the certificates issued by MULTICERT' PKI to:

a) Limit the reliability of the certificates to the uses allowed to them in compliance with that expressed in the corresponding Certificate Policy;

b) Verify the validity of the certificates at the moment of carrying out any operation based on the same;

c) Assume the responsibilities of the correct verification of the digital signatures;

d) Assume the responsibility in proving the validity, revocation or suspension of the certificates in which it trusts;

e) Have full knowledge as to the guarantees and responsibilities applicable for acceptance and use of the certificates in which it trusts and to which it accepts to be subject to.

### 11.6.5 Representation and Guarantees of other Participants

Nothing to remark.

## 11.7 Renouncing Guarantees

MULTICERT's PKI refuses all service guarantees that are not bound by the obligations set forth in this CPS.

## 11.8 Limitation to Obligations

MULTICERT Root CA:

a) shall answer for the damages caused to any person exercising its activity in accordance with Article 26, of the Decree-Law 62/2003;

b) shall answer for the damages caused to subscribers or third parties due to lack or delay of including in the consultation service the validity of the certificates, and revocation or suspension of a certificate, once it has knowledge of it;

c) shall assume all liability before third parties for the actions of the subscriber for functions necessary to provide certification services;

d) The responsibility for the administration / management of the MULTICERT Root CA rests on an objective base and covers all the risks that a private individual may undergo whenever this is a consequence of the normal or abnormal operation of its services;

e) shall only answer for damages caused by misuse of the recognised certificate, when the limits of its possible use have not been clearly consigned on the certificate, in a clear recognized way by third parties;

f) shall not be responsible when a subscriber exceeds the limits listed in the certificate as to its possible uses, in accordance with the conditions set forth and communicated to the subscriber;

g) shall not assume any responsibility in case of loss or damage:

ii) Of the services it provides, in the case of war, natural disasters or any other case of force majeure;

iii) Resulting from the use of certificates when these exceed the limits set forth in the Certificates Policy and corresponding CPS;

iv) Resulting from the undue or fraudulent use of the certificates or CRLs issued by MULTICERT Root CA.

## 11.9 Indemnities

In accordance with the legislation in force.

# 11.10 Termination and Cessation of the Activity

## 11.10.1 Termination

The documents related with MULTICERT's PKI (including this CPS) become effective immediately after they are approved by Management Working Group, and shall only be eliminated or changed upon its order.

This CPS comes into force from the moment it is published in the repository from MULTICERT Root CA.

This CPS shall remain in force while it is not expressly revoked by issuing a new version or by renewing the keys from MULTICERT Root CA, on which moment a new version shall be necessarily drawn up.

## 11.10.2 CPS Substitution and Revocation

The Management Working Group may decide in favour of the elimination or amendment of a document related with MULTICERT's PKI (including this CPS) when:

- Its contents are considered incomplete, inaccurate or erroneous;
- Its contents have been compromised.

In that case, the eliminated document shall be replaced by a new version.

This CPs shall be replaced by a new version with autonomy of the transcendence of the changes carried out within the same, so that it shall be totally applied.

When the CPS is revoked, it shall be removed from the public repository, however it is guaranteed that it will be kept for 20 years.

## 11.10.3 Consequences of the cessation of activity

After the Management Working Group decides in favour of the elimination of the document related to the CE, the Authentication Working Group has 30 working days to submit a replacement document(s) to the approval of the Management Working Group.

The obligations and restrictions established in this CPS, regarding the audits, confidential information, obligations, and responsibilities of MULTICERT's PKI, born while it is in force, shall subsist after substitution or revocation, by a new version in everything that does not oppose it.

# 11.11 Individual Notification and Communication to the Participants

All participants shall use reasonable methods to communicate with each other. These methods may include digitally signed e-mail, fax, signed forms, or other, depending on the criticality and subject of the communication.

# 11.12 Changes

## 11.12.1 Change Procedures

In order to change this document or any of the certificate policies, it is necessary to submit a formal request to the Authentication Working Group indicating (at least):

- The identification of the person who submitted the change request;
- The reason for the request;
- The requested changes.

The Authentication Working Group shall review the request, and if its pertinence is verified, proceeds to the necessary updates to the document, resulting in a new version of the document draft. The new document draft is then made available to all the members of the Working Group and to the involved parties (if any) to allow its scrutiny. Counting from the date it is made available, the different parts have 15 working days to submit their comments. At the end of that period, the Authentication Working Group have another 15 working days to analyse all received comments, and if relevant, incorporate them in the document, after which the document is approved and sent to the Management Working Group for validation and publication, and the final changes become effective.

## 11.12.2 Notification Period and Mechanism

In case the Management Working Group thinks that the changes to the specification may affect the acceptability of the certificates to specific purposes, it shall be communicated to the user of the corresponding certificates that a change was made and that they should consult the new CPS in the repository.

## 11.12.3 Reasons to Change OID

The Authentication Working Group shall determine if the changes to the CPS require a change in the OID of the Certificate Policy or in the URL pointing to the CPS.

In the cases in which, by judgement of the Authentication Working Group, the changes to the CPS do not affect the acceptance of the certificates, an increase in the lower version number of the document and the last Object Identifier number (OID) that represents it shall take place, maintaining the higher version number of the document, as well as the rest of its associated OID. It is not necessary to communicate this type of modifications to the certificate users.

In case the Authentication Working Group finds the changes to the specification might affect the acceptability of the certificates to specific purposes, an increase to the higher version number of the document shall take place and the lowest number shall be placed to zero. The last two numbers of the Object Identifier (OID) that represent it shall also be changed. This type of changes shall be communicated to the certificate users in accordance with that set forth in point 11.12.2.

# 11.13 Dispositions for Solving Disputes

All complaints between users and MULTICERT's PKI shall be communicated by the dispute party to the Accreditation Authority for the purpose to try to solve it between the parties.

For solving any conflict that may arise regarding this CPS, the parties, renouncing to any other courts that may correspond to it, submit themselves to the Civil Litigation Jurisdiction.

# 11.14 Applicable Legislation

The following specific legislation is applicable to the activities of the Certification Authorities:

a) Official Communication no. 27008/2004, from December 14th, published in D.R II, no. 302, from December 28th;

b) Order no. 1350/2004, from October 23rd;

c) Official Communication no. 16445/2004, from July 29th, published in D.R II, no. 190, from August 13th;

d) Notice no. 8134/2004, from July 29th, published in D.R II, no. 190, from August 13th;

e) Regulatory Decree no. 25/2004, from July 15th;

f) Decree-Law no. 290-D/99, from August 2nd with the changes introduced by Decree-Law no. 62/2003, from April 3rd and Decree-Law no. 165/2004, from July 6th;

g) Order no. 1370/2000, published in D.R. no. 211, II series from September 12th;

h) ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI): policy requirements for certification authorities issuing public key certificates, v2.4.1;

i) ETSI TS 101 456: Electronic Signatures and infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, v1.4.3.

j) CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.06

# 11.15 Compliance with the Legislation in force

This CPS is subject to national and European laws, rules, regulations, ordinances, decrees and order including, but not limited to, the restrictions on export or import of *software*, *hardware* or technical information.

It is the responsibility of the Accreditation Authority to ensure the compliance of the applicable legislation listed in section 11.14.

# 11.16 Various Provisions

## 11.16.1 Complete Agreement

All trusting parties totally assume the content of the last version of this CPS.

## 11.16.2 Independence

Should one of more stipulations of this document be or tend to be invalid, null or unclimbable, in legal terms, they shall be considered non-effective.

The previous situation is valid only in those cases in which these stipulations are not considered essential. It is the responsibility of the Accreditation Authority to assess their essentiality.

### 11.16.3 Severity

Nothing to remark.

### 11.16.4 Proceedings (lawyers' fees and giving up rights)

Nothing to remark.

### 11.16.5 Force Majeure

Nothing to remark.

## 11.17 Other Provisions

Nothing to remark.

# 12 List of Definitions and Acronyms

## Definitions

| | |
|---|---|
| **Digital signature** | Advanced electronic signature modality based on an asymmetric cryptographic system made up by an algorithm or series of algorithms, with which is generated an exclusive and interdependent key pair, one of which is private and another public, and which allows the subscriber to use the private key to declare authorship of the electronic document to which the signature has been added and agreement with its content, and the recipient to use the public key to check if the signature created with the corresponding private key and if the electronic document was changed after the signature was added; |
| **Electronic signature** | Is the result of electronic processing of data susceptible of constituting the object of individual and exclusive right and used to make the authorship of the electronic document known. |
| **Advanced electronic signature** | Electronic signature that fulfils the following requirements:<br>i) Identifies unequivocally the subscriber as author of the document;<br>ii) Its addition on the document depends only on the will of the subscriber;<br>iii) Created with means which the subscriber can maintain under its exclusive control;<br>iv) Its connection with the document enables detecting all and any change resulting from its content. |
| **Qualified electronic signature** | Digital signature or other advanced electronic signature that satisfies safety demands identical to those of digital signatures based on a qualified certificate and created through a secure device for signature creation. |
| **Accreditation Authority** | Competent entity for the accreditation and supervision of the Certification Authorities. |
| **Certificate** | Electronic document that connects the data for verifying the signature of its subscriber and confirms the subscriber identity. |
| **Qualified Certificate** | Certificate holding the elements referred on article 29 from DL 62/2003 [7], and it is issued by a Certification Authority complying with all the requirements defined in article 24 of DL 62/2003. |
| **Private key** | Element of asymmetric key pairs meant to be known only to its subscriber, on which the digital signature is added on the electronic document, or which deciphers a previously enciphered electronic document, with the corresponding public key. |

| | |
|---|---|
| **Public key** | Element of asymmetric key pairs meant to be released, with which the digital signature added on the electronic document by the subscriber of the asymmetric key pair is witnessed or by which an electronic document to be transmitted to the subscriber of the same key pair is enciphered. |
| **Accreditation** | Act by which it is recognized, to an entity requesting it and which exercises activities as Certification Authority, as fulfilling the requirements defined in the present diploma for the purposes therewith foreseen. |
| **Data for creating a signature** | Unique set of data, such as private keys, used by the subscriber to create an electronic signature. |
| **Data for verifying a signature** | Set of data, such as public keys, used to verify an electronic signature. |
| **Device for signature creation** | Software or equipment device used to make the treatment of data for signature creation possible; |
| **Safe device for signature creation** | Device for creation of signatures that ensures, through appropriate technical and procedural means that:<br>i) The data necessary to create a signature used in generating a signature can only occur one sole time and that confidentiality of that data is assured;<br>ii) The data necessary to create a signature used to generate a signature cannot, with a reasonable degree of safety, be deduced from other data and that the signature is protected against falsifications carried out through the technologies available;<br>iii) The data necessary to create a signature used to generate a signature may be effectively protected by the subscriber against the illegitimate use by third parties;<br>iv) Data that require a signature are not modified and may be presented to the subscriber before the signature process. |
| **Electronic document** | Document elaborated through data electronic processing. |
| **E-mail** | Identification of the appropriate computer equipment to receive and store electronic documents. |
| **Time stamp** | Data structure that connects the electronic representative of a *datum* to a particular date/time, making evidence that the *datum* existed at that date/time. |
| **Trusting party** | Recipient of a time stamp that trusts in the same. |
| **TSA system** | Composition of IT products and components, organized in order to support the supply of chronological validation services. |
| **UTC (*Coordinated Universal*** | Time scale based on the second as defined in *ITU-R Recommendation TF.460-* |

| | |
|---|---|
| ***Time*)** | *5* [10]. |
| **UTC(k)** | Time scale supplied by the laboratory "k" ensuring ±100 ns in relation to UTC (according to *ITU-R Recommendation TF.536-1* [11]) |
| **Chronological validation** | Statement of a EVC attesting the date and time for creation, expedition or reception of an electronic document. |

# Acronyms

| | |
|---|---|
| **ANS** | *National Security Authority* |
| **ANSI** | *American National Standards Institute* |
| **C** | *Country* |
| **CA** | *Certification Authority* |
| **CN** | *Common Name* |
| **CRL** | Certificate Revocation List |
| **DL** | Decree-Law |
| **DN** | *Distinguished Name* |
| **CPS** | Certification Practices Statement |
| **RD** | Regulatory Decree |
| **CA** | Certification Authority |
| **DCE** | Document Certification Authority |
| **RE** | Registration Entity |
| **GMT** | Greenwich Mean Time |
| **LRC** | See CRL |
| **MAC** | *Message Authentication Codes* |
| **O** | *Organization* |
| **OCSP** | *Online Certificate Status Protocol* |
| **OID** | Object Identifier |
| **CP** | Certificate Policy |
| **PKCS** | *Public-Key Cryptography Standards* |
| **PKI** | Public Key Infrastructure |
| **SHA** | *Secure Hash Algorithm* |
| **SGCVC** | *System for Managing the Certificate Life Cycle* |
| **SSCD** | *Secure Signature-Creation Device* |
| **TSA** | Time-Stamping Authority (the same as EVC) |

# Approval

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.

Assinado de forma digital por [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
DN: c=PT, o=MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A., ou=Certificado para pessoa colectiva - Assinatura Qualificada, title=Procurador com poderes indicados na procuração emitida em 16/10/2013 - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, serialNumber=505767457, cn=[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
Dados: 2015.10.05 17:12:09 +01'00'