multicert
Engineering for digital security

Subordinate CA Policy

Policies

MULTICERT_PJ.ECRAIZ_405_en

Project Identification: Multicert Root CA

CA Identification: Multicert Root CA

Rating: Public

Version: 1.0

Date: 24/07/2017

Multicert, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 - 2740-266 Porto Salvo – Oeiras
Telephone: +351 217 123 010 Fax: +351 217 123 011

Document Identification: MULTICERT_PJ.ECRAIZ_405_en

Keywords: Política de Certificados, EC MULTICERT

Document Type: Policies

Title: Subordinate CA Policy

Original idiom: Português

Publication idiom: English

Rating: Public

Date: 24/07/2017

Current version: 1.0

Project Identification: Multicert Root CA

CA Identification: Multicert Root CA

Client:

Version History

Version Nr.	Date	Details	Author(s)
1.0	24/07/2017	Initial version for approval	Multicert S.A.

Related Documents

Document ID	Details	Author(s)
Multicert_PJ.ECRAIZ_24.1.1_0001_pt.doc	Multicert Root Certification Authority Certification Practices Statement	Multicert S.A.

1.1 Executive Abstract

Resulting from the implementation of several public and private programs to promote information and communication technologies and introduce new relationship processes into society, between citizens, companies, non-governmental organizations and the State, in order to strengthen the information society, eGovernment and electronic trade, Multicert Root Certification Authority supplies the necessary mechanisms for the issuance of certificates for Subordinate Certification Authorities, constituting a hierarchy of trust, which promotes the electronic security of the titleholder of the digital certificate issued within this hierarchy.

Multicert Root Certification Authority establishes a structure of electronic trust, which enables carrying out secure electronic transactions, strong authentication, a means of electronically signing transactions or electronic information and documents, assuring their authorship, integrity, and non-repudiation, as well as the confidentiality of the transactions or information.

This document defines the Certificate Policy in use for issuing certificates for Subordinate Authorities, which complements and is in accordance with Multicert Root Certification Authority Certification Practices Statement (CPS)[1].

Renato Isaias Rodrigues Portela
Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.11.21 17:38:14 Z

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.11.23 08:11:31 Z

[1] Cf. Multicert_PJ.ECRAIZ_24.1.1_0001_pt.doc, 2015, Multicert Root Certification Authority Certification Practices Statement.

Table of Contents

2 Introduction

This is a Certificate Policy (CP) document, whose purpose is the definition of a set of policies and data for the issuance and validation of certificates, and for the assurance of their reliability. It is not meant to name legal rules or obligations, but to inform. Therefore, this document is intended to be simple, straightforward, and understood by a wide public, including people with no technical or legal knowledge.

This document describes the certificate policy for the issuance and management of the Subordinate CA certificate, issued by Multicert Root CA.

The certificates issued by Multicert Root CA contain a reference to the CP, so that the Relying Parties and others interested may find information on the certificate and the policies of the entity which issued it.

2.1 Overview

This document meets and complements the requirements imposed by Multicert Root CA Certification Practices Statement (CPS)[1].

2.2 Designation and Identification of the Document

This document is the Multicert Root CA Subordinate CA Certificate Policy. The CP is represented in the certificate by a unique number called "object identifier" (OID). The value of the OID associated with this document is identified in the table below.

This document is identified by the following data:

DOCUMENT INFORMATION	
Document Version	Version 1.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Issuing Date	14/06/2017
Validity	Not applicable
Location	https://pkiroot.multicert.com/index.html

3 Identification and Authentication

3.1 Naming

The naming follows the convention determined by the CPS of MULTICERT Root CA.

3.1.1 Types of names

The certificate of the Subordinate Authority (SubCA) is identified by a unique name (DN – Distinguished Name), that complies with X.500 standard.

In general, the Distinguished Name of the certificate consists of the following components:

Attribute	**Code**	**Value**
Country	C (required)	<Country of nationality of the Subordinate Authority>
Organization	O (required)	<Organization to which the Subordinate Authority belongs>
Organization Unit	OU (optional)	<Area/Department of the Organization to which the Subordinate Authority belongs>
Organization Unit	OU (optional)	<Other Area/Department of the Organization to which the Subordinate Authority belongs>
Common Name	CN (required)	<Name of the Subordinate Authority>

3.2 Subscriber certificate and key pair usage

The certificate titleholders will just and only use their private key for the purpose for which it is meant (as set forth in the certificate's "*Key Usage*" field) and always for legal purposes.

Its use is only allowed:

a) to whom is named in the field "*subject*" of the certificate;

b) according to the conditions defined in sections 2.4.1 and 2.4.2 of Multicert Root Certification Authority Certification Practices Statement;

c) while the certificate is valid and not in the CRL from Multicert Root CA.

4 Certificate and CRL Profiles

4.1 Certificate Profile

The users of a public key have to trust that the associated private key is held by the correct remote titleholder (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 a data structure that makes the connection between the public key and its titleholder. This connection is stated through the digital signature of each certificate by a trusted CE. The CE 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 titleholder.
A certificate has a limited validity period, indicated in its content and signed by the CE. Since the signature of the certificate and its validity may be independently verified by any software that uses certificates, these may be distributed through communication lines and public systems, and may also be stored in the type of storage units more suitable for each type of certificate[2].
The user of a security system that requires the knowledge of the user's public key 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 CE that signed the certificate, as well as the name of the CE and related information (such as the validity period), then there may be required an additional certificate to obtain the public key from the CE 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 CE and the certificates from the CEs which signed this certificate and so on, until reaching the Root CA.

The profile of the subCA certificate is compliant with:

- ITU.T recommendation X.509[3],
- RFC 5280[3],
- Regulation 910/2014 and,
- CABForum Baseline Requirements.

4.1.1.1 Version Number

The "*version*" certificate field describes the version used in its encoding. In this profile, the version used is 3 (three).

[2] cf. RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*
[3] cf. ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

4.1.1.2 Certificate Extensions

The components and extensions defined for X.509 v3 certificates provide methods for associating attributes to users or public keys, as well as for managing the certification hierarchy.

4.2 Certificate Profile

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
tbsCertificate	**Version**	4.1.2.1	v3	m	Certificate version according to the X.509 standard
	Serial Number	4.1.2.2	<Assigned by the CA to each certificate>	m	N.A
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Value MUST match the OID in *signatureAlgorithm* (below)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		Country of the Root CA
	Organization (O)		"Multicert - Serviços de Certificação Electrónica S.A."		Formal name of the Root CA organization
	Common Name (CN)		"Multicert Root Certification Authority <nn>"		<nn> is a sequential value of the Root CA, starting with "01".
	Validity	4.1.2.5		m	Validity of the Certificate MUST use UTC time scale until 2049, using *GeneralisedTime* from then on.

[4] The profile uses the following terminology for each of the field types in the X.509 certificate:
m – mandatory (the field MUST be present)
o – optional (the field MAY be present)
c – critical (the extension is marked critical, which means that the applications using the certificates MUST process this extension).

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	Not Before		<issuing date>		
	Not After		<issuing date + 4139d >	m	By default the validity will be 4139d. However, it may have a different validity as long as it does not exceed the validity of Multicert Root CA
	Subject	4.1.2.6		m	
	Country (C)		<Country of nationality of the Subordinate Authority>	m	
	Organization (O)		<Organization to which the Subordinate Authority belongs>	m	
	Organization Unit (OU)		<Area/Department of the Organization to which the Subordinate Authority belongs>	o	
	Organization Unit (OU)		<Other Area/Department of the Organization to which the Subordinate Authority belongs>	o	
	Common Name (CN)		<Name of the Subordinate Authority>	m	
	Subject Public Key Info	4.1.2.7		m	Used to hold the public key and identify the algorithm with which the key is used (e.g., RSA, DSA or Diffie-Hellman).

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	Algorithm		1.2.840.113549.1.1.1		The *rsaEncryption* OID identifies RSA public keys. *{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}* The *rsaEncryption* OID shall be used in the field *algorithm* with a value of type *AlgorithmIdentifier*. The parameters of the field MUST have ASN.1type NULL for this algorithm identifier.[5]
	subjectPublicKey		<Public Key with *modulus* n of 4096 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		The *key Identifier* is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey BIT STRING* (excluding the tag, length, and number of unused bits)>	m	
	Subject Key Identifier	4.2.1.2	The *key Identifier* is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey BIT STRING* (excluding the tag, length, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL.

[5] *cf.* RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
					Gives the type of use of the certificate (KeyCertSign; CRLSign).
	Digital Signature		"0" selected		
	Non Repudiation		"0" selected		
	Key Encipherment		"0" selected		
	Data Encipherment		"0" selected		
	Key Agreement		"0" selected		
	Key Certificate Signature		"1" selected		
	CRL Signature		"1" selected		
	Encipher Only		"0" selected		
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.7	m	Identifier of Multicert Root CA Certification Practices Statement

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	policyQualifiers		**policyQualifierID:** 1.3.6.1.5.5.7.2.1 **cPSuri:** http://pkiroot.multicert.com/	m	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.1.2	m	Certificate Policy for Subordinate Authorities
	policyQualifiers		**policyQualifierID:** 1.3.6.1.5.5.7.2.2 **cPSuri:** http://pkiroot.multicert.com/		
	policyIdentifier		2.5.29.32.0		Any policy
	Basic Constraints	4.2.1.9		c	This extension is marked CRITICAL.
	CA		TRUE		
	Path Length Constraint		3		
	CRLDistributionPoints	4.2.1.13		m	
	distributionPoint		http://pkiroot.multicert.com/crl/root_mc_crl.crl	m	
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.36.1.5.5.7.48.1	m	OID Value: 1.36.1.5.5.7.48.1 (id-ad-ocsp)

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	accessLocation		http://ocsp.multicert.com/ocsp	m	
	accessMethod		1.36.1.5.5.7.48.2	o	OID Value: 1.36.1.5.5.7.48.2 (id-ad-caissuers)
	accessLocation		http://pkiroot.multicert.com/cert/MCRootCA.cer	o	
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	MUST contain the same algorithm identifier OID of the *signature* field in the sequence tbsCertificate. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	Signature Value	4.1.1.3	<contains the digital signature issued by the CA>	m	By generating this signature, the CA certifies the binding between the public key and the titleholder (*subject*) of the certificate.

4.2.1 Algorithm OID

The "*signatureAlgorithm*" field of the certificate contains the OID for the cryptographic algorithm used by the CA to sign the certificate: 2.16.840.113549.1.1.11 (sha-256WithRSAEncryption[6]).

4.2.2 Name Forms

As defined in section **Error! Reference source not found.**.

4.2.3 Name Constraints

To guarantee full interoperability between the applications that use digital certificates, it is advisable (not mandatory) to use only unaccented alphanumeric characters, space, underscore, minus sign and full stop ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') in X.500 Directory entries.

4.2.4 Certificate Policy OID

The extension "*certificate policies*" contains a sequence of one or more informative terms about the policy, each consisting in a policy identifier and optional qualifiers.

The optional qualifiers ("*policyQualifierID*: 1.3.6.1.5.5.7.2.1" and "*cPSuri*") point to the URI where the Certification Practices Statement with the OID identified by the "*policyIdentifier*" can be found. The optional qualifiers ("*policyQualiflierID*: 1.3.6.1.5.5.7.2.2" and "*userNotice explicitText*") point to the URI where the Certificate Policy with the OID identified by the "*policyIdentifier*" can be found (i.e., this document).

4.2.5 Usage of *Policy Constraints* extension

Nothing to remark.

4.2.6 Policy qualifier syntax and semantics

The extension "*certificate policies*" contains a type of policy qualifier to be used by the certificate issuers and the writers of the certificate policy. The type of qualifier is the "*cPSuri*", which contains a pointer, in the form of URI, to the Certification Practices Statement published by the CA; and the "*userNotice explicitText*", which contains a pointer, in the form of URI, to the Certificate Policy.

[6] sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} }

4.2.7 Processing semantics for the *Certificate Policies* critical extension

Nothing to remark.

4.3 Certificate Revocation List Profile

When a certificate is issued, it is expected to be in use for its entire validity period. However, several circumstances may cause a certificate to become invalid before the expiration of its validity period. Such circumstances include change of name, change of association between the subject and the certificate data (for example, an employee who terminates employment) and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA has to revoke the certificate[7].

The protocol X.509 defines a method of certificate revocation, which involves the periodic issuing, by the CA, of a signed data structure called a Certificate Revocation List (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by the CA and made freely available in a public repository. Each revoked certificate is identified in the CRL by its serial number. When an application uses a certificate (e.g., for verifying a remote user's digital signature), that application not only verifies the certificate signature and validity; it also obtains the most recent CRL and checks if the serial number of the certificate is not in it. Note that a CA issues a new CRL on a regular periodic basis.

For Subordinate Authorities, this list is called CARL (*Certification Authority Revocation List*), which is issued every 3 months.

The CARL profile complies with the CRL profile indicated in this Policy.

[7] cf. RFC 5280. 2008, *Internet* X.509 *Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile*.

5 Identification and Authentication

5.1 Validating Identity during initial registration

Eligible as potential Subordinate Certificate Authorities of Multicert Root CA are those entities (natural or collective accredited persons) that create or provide means to create the keys, issue digital certificates, ensure the respective advertising and provide other services connected to digital signatures.

5.1.1 Method to Prove Possession of the Private Key

As a method to prove possession of the private key, Multicert Root CA verifies if the Certification Authority to be accredited holds the private key corresponding to the public key for which the digital certificate was requested. The use of the *Certificate Management Protocol* (CMP) defined in RFC 4210 is considered an acceptable mechanism as proof method. It is also to be considered that the possession of the private key by the issuer of the certificate application can be proven, since this certificate request format is signed by the private key.

5.1.2 Authentication of the Identity of a Collective Person

The certificate issuance request made by a Subordinate Authority to Multicert Root CA must be accompanied by the following documents, whenever legally verified:

- Statutes of the collective person and, in the case of a company, partnership agreement or, in the case of a natural person, the corresponding identification and address;
- In the case of a company, a list of all shareholders, specifying their respective interests, as well as a list of the members of the management and supervisory bodies, and, in the case of a public company, a list of all shareholders with significant direct or indirect interests;
- Evidence of the asset base and financial resources available and, in particular, in the case of a company, full payment of share capital;
- Name of the security auditor for each type of certificate issued and corresponding declarations of compliance, certified by an Entity accredited for this purpose;
- Proof of insurance contract, valid for adequate coverage of civil liability arising from the certification activity.

5.1.3 Non-verified subscriber information

Nothing to remark.

5.1.4 Validation of Authority

Nothing to remark.

5.1.5 Criteria for affiliation

In the processes concerning affiliation agreements, the following documentation will be analyzed:

a) The Certificate Policy;
b) Declaration of Compliance issued by an entity accredited for the purpose, according to 8.2 *Baseline Requirements Certificate Policy* and/or according to Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.
c) Acceptance of protocol provided by Multicert Root CA, Multicert Root CA Certification Practices Statement and this document.

5.2 Identification and Authentication for revocation request

Any entity can request the revocation of its certificate by the following reasons:

- Function Termination;
- Compromise of the Keys.

In any of the situations, the revocation request is made formally obeying the statutes that bind the entity.

Any entity integrated in Multicert's domain can request the revocation of a certain certificate, when there is knowledge or suspicion of compromise of the titleholder's private key. In this case, the requesting entity shall carry out the request accompanied by evidence, in case of knowledge, or motivations that support the suspicion of private key compromise.

Multicert will immediately assess the request and, within 5 working days, it will issue a verdict to the requesting entity, as well as the entity holding the certificate to be revoked.

Multicert may also determine the revocation of its Subordinate Authorities before the following scenarios:

- Absence of declaration of compliance;

- Identification of issuance of fraudulent certificates;
- Identification of issuance of certificates which do not comply with the applicable legislation and/or international standards.

For each situation, Multicert will immediately inform the Subordinate Authority, agreeing the time to solve it, according to the criticality level.

Multicert shall revoke the keys whenever the reason is Key Compromise and this is duly proven.

6 Certificate life-cycle operational requirements

6.1 Certificate Application

It is only possible to carry out the certificate request for a Subordinate CA after acceptance of the conditions imposed by Multicert Root CA, namely acceptance of a protocol which will be provided, reading this document and the subsequent authorization of operation of the Subordinate CA by Multicert Root CA.

Once the acceptance is formalized, a **Subordinate CA Certificate Issuance Form** will be made available by Multicert to the applicant, and this must be completed and signed by the legal representative(s) of the entity.

6.2 Certificate Issuance

6.2.1 Procedures for issuing a certificate

The issuance of the certificate is performed through a ceremony that is held within the high security zone of Multicert Root CA, after acceptance of a subscription agreement, in which are present:

- 4 Members of Multicert PKI Working Groups, since the function segregation does not allow the presence of an inferior number of elements;
- Any observers accepted simultaneously by the Management Group of Multicert Root CA and the representatives of the requesting subordinate Authority.

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

a) Identification and authentication of all the people present, ensuring that the representative(s) of the requesting Subordinate CA and the members of the Working Groups have the necessary powers for the acts to be performed;

b) Representative(s) of the requesting Subordinate CA deliver the certificate request in PKCS#10 format, together with the **Subordinate CA Certificate Issuance Form**, duly completed and signed, to the members of Multicert Root CA Working Group. The form is dated and

signed by the members of the Working Group, who return it to the representative(s) of the requesting subordinate Authority;

c) The members of the Working Group perform the starting procedure of processing Multicert Root CA and issue the certificate (corresponding to the PKCS#10 provided in the CD/DVD) in PEM format;

d) The members of the Working Group store the certificate in PEM format in a CD/DVD and complete and sign the Subordinate CA Certificate Receipt Form;

e) The members of the Working Group request the signature of the **Subordinate CA Certificate Receipt Form** to the representative(s) of the subordinate Authority and deliver the CD/DVD along with the issued certificate;

f) The issuing ceremony is completed with the execution of Multicert Root CA finishing processing procedure by the members of Multicert Root CA Working Group.

The subordinate Authority has three working days after receiving the certificate to carry out the validations that they deem appropriate and formalize its acceptance, by completing the **Subordinate CA Certificate Acceptance Form,** returning it duly completed and signed to the elements of Multicert Root CA Working Groups.

The certificate may only be made available to the end user after an agreement has been signed between the entities involved (namely those that benefit, directly or indirectly, from its hierarchy).

The issued certificate comes into force after its formal acceptance by the subordinate Authority.

6.2.2 Notification of certificate issuance to the subscriber

The issuance of the certificate is performed according to the previous section, thus the certificate subscriber is notified upon its delivery.

6.3 Certificate Acceptance

6.3.1 Procedures for accepting the certificate

The certificate acceptance is performed according to chapter 6.2.1 paragraph e).

6.3.2 Publication of the certificate

Multicert will publish the certificates issued to subordinate Authorities through its public repository pki.multicert.com in its Certification Practices Statement.

6.3.3 Notification of certificate issuance to other entities

Multicert will report the issuance of certificates to subordinate Authorities by publishing new versions of Multicert Root CA CPS.

6.4 Certificate and key pair usage

6.4.1 Certificate and private key usage by the titleholder

The private key associated to the certificate issued within the scope of this policy is used just and only for the purpose for which it is meant (as set forth in the certificate's "*keyUsage*" field) and always for legal purposes, established in the scope of this policy.

Its use is only allowed:

a) to the Subordinate Authority for which the certificate was issued;

b) while the certificate is valid and not in the CRL from Multicert Root CA.

6.4.2 Certificate and public key usage by the relying parties

As in section 5.3.5 of Multicert Root Certification Authority Certification Practices Statement.

6.5 Certificate renewal with generation of a new key pair

The renewal of certificate keys (*certificate re-key*) is the process in which a titleholder (or legal representative) generates a new key pair and submits the request for issuance of a new certificate that certifies the new public key. This process, within the scope of this Certificate Policy, is designated by certificate renewal with generation of a new key pair.

This section complies with section 5.2 of Multicert Root CA Certification Practices Statement.

6.5.1 Circumstances for renewing a certificate, generating a new key pair

As in section 5.5.1 of Multicert Root CA Practices Statement document.

6.5.2 Who may request certification of a new public key

As in section 5.1 of Multicert Root CA Practices Statement document.

6.5.3 Processing the certificate renewal request with generation of a new key pair

As in section 5.2. of Multicert Root CA Practices Statement document.

6.5.4 Notification of new certificate issuance to subscriber

As in section 6.2.2 of this document.

6.5.5 Procedures for accepting a renewed certificate with generation of a new key pair

As in section 5.3.1 of Multicert Root CA Practices Statement document.

6.5.6 Publication of a renewed certificate with generation of a new key pair

As in section 5.3.2 of Multicert Root CA Practices Statement document.

6.5.7 Notification of issuance of renewed certificate to other entities

As in section 5.3.1 of Multicert Root CA Practices Statement document.

6.6 Certificate suspension and revocation

As in section 5.7 of Multicert Root CA Practices Statement document.

7 Audit and Compliance assessments

All Certificate Authorities integrated in Multicert Root CA's hierarchy must necessarily create their own Certification Practices Statements in accordance with the minimum requirements defined in this document, as well as those defined in Multicert Root CA Certification Practices Statement.

7.1 Frequency or reason for the audit

According to the previous point, the various entities are audited in the following situations:

a) In the process of integration in Multicert Root CA;

b) Annually;

c) At any time, without prior notice.

Section 9.2 of Multicert Root CA Certification Practices Statement clarifies the regularity and the occurrence of the various audits.

7.2 Identity and Qualifications of the auditor

The auditor is a person or organization with recognized suitability, holding proved experience and qualifications in the field of security of information and information systems, public key infrastructures and duly accredited by an Accreditation Authority under the Regulation 910/2014.

7.3 Scope of the audit

All entities that directly or indirectly carry out certification activities under the terms of this policy are audited.

The audits must be carried out in accordance with what is stipulated in regulation 910/2014 and applicable legislation, wherein Multicert receives annually a Declaration of Compliance from its subordinate Authorities. Likewise, the Subordinated Authorities must undergo a penetration test, annually, which includes all services made available.

In addition to compliance audits, Multicert may carry out further inspections and investigations to ensure compliance of the Certification Authorities integrated in the Multicert PKI with the applicable national legislation as well as international standards. The execution of these internal audits, inspections and investigations may be delegated to an external audit entity.

8 Other situations and Legal Matters

8.1 Fees

8.1.1 Fees for Certificate Issuance or Renewal

As defined in section 11.1.1 of Multicert Root CA Certification Practices Statement.

8.1.2 Fees for Certificate Access

Nothing to remark.

8.1.3 Fees for Access to Information on the status of the Certificate or Revocation

As defined in section 11.1.3 of Multicert Root CA Certification Practices Statement.

8.1.1 Reimbursement policy

Nothing to remark.

8.1.2 Fees for other Services

As defined in section 11.1.4 of Multicert Root CA Certification Practices Statement.

8.1.3 Reimbursement policy

Nothing to remark.

9 Financial Responsibility

9.1 Insurance Coverage

Multicert Root CA Subordinate Authorities must comply with the legislation in force in relation to third-party liability insurance.

9.2 Other Insurance

Nothing to remark.

10 Confidentiality of the Information Processed

As in section 11.3 of Multicert Root CA Certification Practices Statement.

10.1 Privacy of Personal Data

As in section 11.4 of Multicert Root CA Certification Practices Statement.

10.2 Intellectual Property Rights

As in section 11.5 of Multicert Root CA Certification Practices Statement.

10.3 Representations and guarantees

10.3.1 Representation and guarantees of Certification Authorities

The CAs of Multicert PKI hierarchy are 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 X.509 standard;
e) Issue certificates that are compliant with the information known at the time they are 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 titleholder;
g) Use reliable systems and products that are protected against all changes and which ensure the technical and cryptographic safety of the certification processes;
h) Use reliable systems to store recognized certificates, that enable proving their authenticity and prevent unauthorized 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 its CPS and publish the revoked certificates on the CRL of its repository, with the frequency stipulated in its CPS;

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

n) Notify with the necessary speed the certificate titleholders, by e-mail, in case the CA revokes or suspends the certificates, indicating the reason which led to this action;

o) Collaborate with the audits performed by Multicert Root CA;

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 provisions in section 5.7.10 of Multicert Root CA CPS;

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

t) Have a properly defined plan for Termination of service;

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

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

w) Act in accordance with ETSI EN 319 411-1, ETSI EN 319 411-2 and the CabForum Requirements (each one, as amended and rectified periodically),

x) Ensure that the Certificate profiles issued by the Affiliate and Sub-Affiliates comply with:

   a. ETSI EN 319 412-2 or ETSI EN 319 412-3, for Qualified Certificates and

   b. for Authentication Certificates, only *keyUsage digitalSignature* and EKU *clientAuth*.

y) Carry out all the validation required by the Sector Standards before issuing the Certificate,

z) Issue each type of certificate from a separate SubCA,

aa) Ensure that all the Certificates contain an *extendedKeyUsage* value different from *anyExtendedKeyUsage*.

10.3.2 Representation and guarantees of the Registration Authorities

Nothing to remark.

10.3.3 Representation and guarantees of the titleholders

As in section 11.6.3 of Multicert Root CA Certification Practices Statement.

10.3.4 Representation and guarantees of the trusting parties

As in section 11.6.4 of Multicert Root CA Certification Practices Statement.

11 List of Definitions and Acronyms

11.1 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 asymmetric key pair, one of which is private and another public, and which allows the titleholder 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 was created with the corresponding private key and if the electronic document was changed after the signature was added.
Electronic signature	It 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: i) Identifies unequivocally the titleholder as author of the document; ii) Its addition on the document depends only on the will of the titleholder; iii) Created with means which the titleholder can maintain under its exclusive control; 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 modality 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 which connects the data for verifying the signature of its titleholder and confirms the titleholder's identity.

Qualified certificate	Certificate holding the elements referred on article 29 from DL 62/2003 [7] and which 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 pair meant to be known only by its titleholder, through which the digital signature is added on the electronic document or an electronic document previously enciphered with the corresponding public key is deciphered.
Public key	Element of asymmetric key pair meant to be released, with which the digital signature added on the electronic document by the titleholder of the asymmetric key pair is verified or by which an electronic document to be transmitted to the titleholder of the same key pair is enciphered.
Accreditation	Act by which it is recognized, to an entity requesting it and which exercises activity as Certification Authority, the fulfilment of 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 titleholder to create an electronic signature.
Date 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 which ensures, through appropriate technical and procedural means, that: i) Data necessary to create a signature, used in generating a signature, can only occur one time and that confidentiality of that data is assured; ii) 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; iii) Data necessary to create a signature, used to generate a signature, may be effectively protected by the titleholder against the illegitimate use by third parties; iv) Data that require a signature are not modified and may be

	presented to the titleholder 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 organised in order to support the supply of chronological validation services.
UTC (*Coordinated Universal Time*)	Time scale based on the second as defined in *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Time scale supplied by the laboratory "k" which ensures ±100 ns in relation to UTC (according to *ITU-R Recommendation TF.536-1* [11])
Chronological validation	Statement of an EVC attesting the date and time for creation, expedition or receipt of an electronic document.

11.2 Acronyms

ANSI	American National Standards Institute
C	Country
CA	Certification Authority (the same as CE)
CN	Common Name
CRL	Certificate Revocation List
DL	Decree-Law
DN	Distinguished Name
CPS	Certification Practices Statement
RD	Regulatory Decree

CA	Certification Authority
DCA	Document Certification Authority
RA	Registration Authority
GMT	Greenwich Mean Time
GNS	*Gabinete Nacional de Segurança* (National Security Office)
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)