multicert

Engineering for digital security

MULTICERT Root CA Certificate Policy

Policy

MULTICERT_PJ.ECRAIZ_24.1.2_0001_en.doc

Project Identification: EC Raiz da MULTICERT

CA Identification: MULTICERT Root CA

Rating: Public

Version: 2.0

Date: 09/07/2014

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

Document Identifier: MULTICERT_PJ.ECRAIZ_24.1.2_0001_en.doc

Key Words: PC, Política, Certificado

Document Type: Política

Title: MULTICERT Root CA Certificate Policy

Original Language: Portuguese

Language of Publication: English

Rating: Público

Date: 09/07/2014

Current Version: 2.0

Project Identification: EC Raiz da MULTICERT

CA Identification: MULTICERT Root CA

Client: ----

Version History

Version Nr.	Date	Details	Author(s)
1.0	30/03/2014	Approved Version	MULTICERT S.A.
1.1	26/06/2014	change of address	MULTICERT S.A.
2.0	09/07/2014	Approved Version	MULTICERT S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.pdf	Certification Practices Statement	MULTICERT S.A.
MULTICERT_PJ.ECRaiz_24.1.13_0001_pt.pdf	Principle Disclosure Statement	MULTICERT S.A.

Executive Summary

Resulting from the implementation of several public and private programmes to promote information and communication technologies and introduce new relationship processes into society – between citizens, companies, non-governmental organisations and the State – in order to strengthen the information society, eGovernment and electronic trade, the digital certificates issued by the Certification Authority MULTICERT, registered in the Accreditation Authority (as provided by European and national laws), supply to the titleholder of the electronic certificate the necessary mechanisms for strong digital authentication of identity, as well as electronic signatures (legal equivalent of handwritten signatures), indispensable for the dematerializing processes.

The infrastructure of MULTICERT CA provides a hierarchy of trust which promotes the electronic security of the titleholder of the digital certificate. MULTICERT CA 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.

MULTICERT Certification Authority is duly registered in the National Security Authority, as provided by European and national laws, this way being legally empowered to issue all types of digital certificates, namely qualified digital certificates (digital certificates with the highest degree of security provided by law).

This document defines the certificate Policy in use for issuing the self-signed certificate of MULTICERT CA, which complements and is in accordance with the Certification Practices Statement of MULTICERT Root CA[1].

Purposes of the Document

The purpose of this document is to define the policies used for the issuance of the self-signed certificate of MULTICERT CA, by MULTICERT Root CA.

Target Public

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

Document Structure

It is assumed that the reader knows the concepts of cryptography, public key infrastructure and electronic signature. Should this not be the case, it is recommended that deeper knowledge as to the previously mentioned concepts and topics be attained before continuing to read this document.

This document complements the Certification Practices Statement of MULTICERT Root Certification Authority1, being assumed that the reader has read its full content before starting to read this document.

Definitions and Acronyms

A list of definitions and acronyms relevant to the reading of this policy is included at the end of the document.

[1] Cf. MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.doc, 2014, Certification Practices Statement by the Root Certifying Entity from MULTICERT.

Table of Contents

1 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 certificates issued by MULTICERT Root Certification Authority 01 (MULTICERT Root CA).

All certificates issued from the hierarchy of MULTICERT Root CA comply with the ETSI TS 102 042 and ETSI 101 456 requirements, concerning the identified certificate policies:

0.4.0.2042.1.1	Advanced Certificate Policy (Individual or Professional)[2]
0.4.0.2042.1.2	Advanced Certificate Policy (Individual or Professional) issued on cryptographic device[3]
0.4.0.2042.1.7	TLS/SSL Certificate Policy with Organization validation[4]
0.4.0.2042.1.6	TLS/SSL Certificate Policy with Domain validation[5]
0.4.0.1456.1.1	Qualified Certificate Policy[6]

The certificates issued from the hierarchy of 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.

Following CEs use this CP:

- MULTICERT Root Certification Authority 01;
- MULTICERT Certification Authority <nnn>[7];
- MULTICERT Trust Services Certification Authority <nnn>[7].

1.1 Overview

This CP meets and complements the requirements imposed by the Certification Practices Statement of MULTICERT Root Certification Authority.

1.2 Designation and Identification of the Document

This document is a Certificate Policy of self-signed MULTICERT Root CA. The CP is represented in a certificate by a unique number called "object identifiers" (OID). The value of the OID associated with this document is 1.3.6.1.4.1.25070.1.1.1.0.1.

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

[2] Referred to as *Normalized Certificate Policy* (NCP) in the ETSI TS 102 042 standard
[3] Referred to as *Extended Normalized Certificate Policy* (NCP+) in the ETSI TS 102 042 standard
[4] Referred to as *Organizational Validation Certificate Policy* (OVCP) in the ETSI TS 102 042 standard
[5] Referred to as *Domain Validation Certificate Policy* (DVCP) in the ETSI 102 042 standard
[6] Referred to as QCP+SSCD (*Qualified Certificate Policy + Secure Signature Creation Device*) in the ETSI TS 101 456 standard
[7] <nnn> is a sequential value starting with "001", in the issuance of the first certificate of this type.

Document Information	
Document Version	Version 1.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.0.1
Issuing Date	30/03/2014
Validity	Not Applicable
Location	http://pkiroot.multicert.com/pol/index_en.html

1.3 Contact

The management of this Certificate Policy is the responsibility of the Policy Group of MULTICERT's PKI.

NAME	Policy Working Group of MULTICERT's PKL
Address:	MULTICERT S.A. Lagoas Park, Edifício 3, Piso 3 2740-266 Porto Salvo Oeiras
E-mail:	grupo_politicas@multicert.com
Webpage:	www.multicert.com
Telephone number:	+351 217 123 010
Fax:	+351 217 123 011

2 Identification and Authentication

2.1 Naming

The naming follows the convention determined by the CPS of MULTICERT Root CA[1].

2.1.1 Types of names

The certificate by MULTICERT Root CA is identified by a unique name (Distinguished Name – DN), that complies with X.500 standard.
The Distinguished Name of the certificate by MULTICERT Root CA consists of the following components:

Attribute	Code	Value
Country	C	PT
Organization	O	MULTICERT – Serviços de Certificação Electrónica, S.A.
Common Name	CN	MULTICERT Root Certification Authority <nn>[8]

2.2 Use of the Certificate and Key Pair by the titleholder

MULTICERT Root Certification Authority is the titleholder of the MULTICERT Root CA's self-signed certificate, using its private key for signing certificates of Subordinate Certifying Entities, signing its Certificate Revocation List (CRL), as well as signing certificates intended for the OCSP[9] service, according to its CPS[1].

[8] <nn> is a sequential value starting with "01", in the issuance of the first certificate of this type.

[9] OCSP – Online Certificate Status Protocol

3 Certificate and CRL Profiles

3.1 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, the certificates 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[10].

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 a 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 zero or more additional certificates from CEs signed by other CEs[10].

The profile of the self-signed root certificate issued by MULTICERT Root CA is compliant with:

- ITU.T recommendation X.509[11];
- RFC 5280[10];
- Applicable legislation, national and European;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6; e
- *ETSI TS 101 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.*

3.1.1 Version Number

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

3.1.2 Certificate Extensions

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

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

3.1.3 Certificate Profile

Certificate Component		Section in RFC 5280	Value	Type[12]	Comments
tbsCertificate	**Version**	4.1.2.1	V3	m	
	Serial Number	4.1.2.2	<assigned by the CA to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Value MUST match the OID in signatureAlgorithm (below)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A."		
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"		<nn> is a sequential value starting with "01" in the issuance of the first certificate of this type.
	Validity	4.1.2.5		m	MUST use UTC time scale until 2049, using *GeneralizedTime* from then on.
	Not Before		<issuing date>		
	Not After		<issuing date + 25 years>		Valid for twenty-five years. Used for signing certificates during the first 12 years of validity (maximum) and renewed (with generation of a new key pair) before reaching 12 years and 6 months of validity.

[12] 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).

	Subject	4.1.2.6	<same as *Issuer*>	m	When the subject is a CE, it must contain the same DN as the Issuer.
	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).
	Algorithm		1.2.840.113549.1.1.11		The rsaEncryption OID identifies RSA public keys. sha256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} 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.[13]
	SubjectPublicKey		<Public key with modulus n of 4096 bits>		
	X.509 v3 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 BIT STRING subjectPublicKey (excluding the tag, length and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL
	Digital Signature		"0" selected		

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

	Non Repudiation		"0" selected		
	Key Encipherment		"0" selected		
	Data Encipherment		"0" selected		
	Key Agreement		"0" selected		
	Key Certificate Signature		"1" selected		For signature of certificates
	CRL Signature		"1" selected		For signature of CRLs
	Encipher Only		"0" selected		
	Decipher Only		"0" selected		
	Basic Constraints	4.2.1.9		mc	This extension is marked CRITICAL
	CA		TRUE		
	Path length		none		
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same algorithm identifier OID of the *signature* field in the sequence tbsCertificate. 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 subject of the certificate.

3.1.4 Algorithm OID

The "*signatureAlgorithm*" certificate field contains the OID for the cryptographic algorithm used by the CA to sign the certificate: 1.2.840.113549.1.1.11(sha256WithRSAEncryption[14])[13].

3.1.5 Name Forms

As defined in section 2.1.

3.1.6 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. The usage of accented characters will be the sole responsibility of MULTICERT's PKI Management Working Group.

3.1.7 Certificate Policy OID

The "*certificate policies*" extension is not active in the self-signed certificate of MULTICERT Root CA.

3.1.8 Usage of Policy Constraints Extension

Nothing to remark.

3.1.9 Policy Qualifier Syntax and Semantics

Nothing to remark.

3.1.10 Processing Semantics for the Critical Certificate Policies Extension

Nothing to remark.

3.2 Certificate Revocation List (CRL) 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.[10]

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

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

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.

The CRL profile conforms to:

- ITU.T Recommendation X.5094;
- RFC 52803 and,
- Applicable legislation, national and European.

3.2.1 Version Number

The "*version*" CRL field describes the version used in encoding the CRL. In this profile, the version used is 2 (two).

3.2.2 MULTICERT ROOT CA CRL Base Profile

The components and extensions defined for X.509 v2 CRLs provide methods for associating additional attributes to CRLs.

CRL Component		Section in RFC 5280	Value	Type	Commentaries
tbsCertList	**Version**	5.1.2.1	1	m	Version v2 (the integer value is 1).
	Signature	5.1.2.2	1.2.840.113549.1.1.11	m	Contains the algorithm identifier used for signing the CRL. Value MUST match the OID in *signatureAlgorithm* (below)
	Issuer	5.1.2.3		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A."		
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"		
	thisUpdate	5.1.2.4	<CRL issuing date>	m	Implementations MUST use UTC time scale until 2049, using *GeneralizedTime* from then on.
	nextUpdate	5.1.2.5	<CRL next issuing date = thisUpdate + N>		This field indicates the date by which the next CRL will be issued. The next CRL may be issued before the indicated date, but it will not be issued after it. The CRL issuers SHALL issue CRLs with a *nextUpdate* time equal to or later than all previous CRLs. Implementations MUST use UTC time scale until 2049, using *GeneralizedTime* from then on. N will be maximum 4 months.
	revokedCertificates	5.1.2.6	<list of revoked certificates>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key	5.2.1		o	

	Identifier				
	keyIdentifier		<The key identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING *subject key identifier* of the issuer certificate (excluding the tag, length and number of unused bits)>	m	
	CRL Number	5.2.3	<unique increasing sequence number>	m	
	Issuing Distribution Point	5.2.5		c	
	DistributionPointName		**http://pkiroot.multicert.com/crl/root_mc_crl.crl**		
	CRL Entry Extensions	**5.3**			
	Reason Code	5.3.1		o	Value must be one of the following: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 – Compromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same algorithm identifier OID used in the *signature* field in the sequence tbsCertificate. OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)

					rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	Signature Value	5.1.1.3	<contains the digital signature issued by the CA>	m	Contains the digital signature calculated over the *tbsCertList*.

3.3 OCSP 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, the certificates may be distributed through communication lines and public systems, and may also be stored in any type of storage units[15].

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 a 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 zero or more additional certificates from CEs signed by other CEs.

The profile of the OCSP online Validation Certificates is compliant with:

– ITU.T recommendation X.509[16];

– RFC 5280[15] **Error! No bookmark name given.** and

– Other standards and applicable legislation.

3.3.1 Version Number

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

3.3.2 Certificate Extensions

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

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

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

Certificate Component		Section in RFC 3280	Value	Type [17]	Commentaries
tbsCertificate	**Version**	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<assigned to each certificate by the CA>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Value MUST match the OID in *signatureAlgorithm* (below)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A."		
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"		
	Validity	4.1.2.5		m	MUST use UTC time scale until 2049, using *GeneralizedTime* from then on.
	Not Before		<issuing date>		
	Not After		<issuing date + 1.900 days>		Validity of approximately 5 years and two months. Used to sign OCSP responses during the first month of the validity period and renewed (with generation of a new key pair) after the first month of the validity period.
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A"		

[17] 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).

	Organization Unit (OU)		"Revocation Status Services"		
	Serial Number (SN)		<nnnnnn>		<nnnnnn> is a sequential value starting with "01" in the issuance of the first certificate of this type.
	Common Name (CN)		"OCSP Validation Service		
	Subject Public Key Info	4.1.2.7		m	Used to contain the public key and identify the algorithm with which the key is used (e.g., RSA, DSA or Diffie-Hellman)
	algorithm		1.2.840.113549.1.1.11		The OID rsaEncryption identifies RSA public keys. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}[18] The rsaEncryption OID shall be used in the field *algorithm* with a value of type *AlgorithmIdentifier*. The parameters of the field MUST have ASN.1 Type NULL for this algorithm identifier.[18]
	subjectPublicKey		<Public Key with modulus n of 2048 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 256-bit SHA-256 hash of the value of the BIT STRING *subjectKeyIdentifier* of the issuer certificate (excluding the tag, length, and number of unused bits)>	m	

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

	Subject Key Identifier	4.2.1.2	<The *key Identifier* is composed of the 256-bit SHA-256 hash of the value of the BIT STRING *subjectPublicKey* (excluding the tag, length, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL.
	Digital Signature		"1" selected		
	Non Repudiation		"1" selected		
	Key Encipherment		"0" selected		
	Data Encipherment		"0" selected		
	Key Agreement		"0" selected		
	Key Certificate Signature		"0" selected		
	CRL Signature		"0" selected		
	Encipher Only		"0" selected		
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	Identifier of the Certification Practices Statement of MULTICERT Root CA.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pkiroot.multicert.com/pol/index.html	o	OID Value: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) OID Description: "The cPSuri qualifier contains a pointer to the Certification Practices Statement published by the CA. The pointer is in the form of a URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)

	policyIdentifier		2.16.620.1.1.1.2.4.0.1.6	m	Identifier of the OCSP online Validation Certificates Policy issued by the Citizen CA.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.2 *userNotice explicitText*: "http://pkiroot.multicert.com/pol/index.html"	o	OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) OID Description: "*User notice* is intended for display to a relying party when a certificate is used" (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	Basic Constraints	4.2.1.10		c	This extension is marked CRITICAL.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13	1.3.6.1.5.5.7.3.9	o	OID Description: Indicates that the private key corresponding to the X.509 certificate may be used to sign OCSP responses.
	OCSPNocheck	-	NULL	o	It is not an extension defined in RFC 3280. Defined in http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.48.1.5.html, this extension shall be included in an OCSP signature certificate. This extension shows the OCSP client that this signature certificate may be reliable, even though it doesn't validate by the OCSP server (since the response would be signed by the OCSP server and the client would have to validate again the status of the signature certificate).
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	

	accessMethod		1.3.6.1.5.5.7.48.1	o	OID value: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) OID Description: *Online Certificate Status Protocol*
	accessLocation		http://ocsp.multicert.com/ocsp/	o	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same algorithm identifier OID as 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)}[18]
	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 subject of the certificate.

4 Identification and Authentication

4.1 Validating Identity during Initial Registration

4.1.1 Method to Prove Possession of Private Key

In the self-signed certificate of MULTICERT Root CA, the proof of possession of the private key will be guaranteed through physical presence of the various relevant Working Groups, in the issuing ceremony of that type of certificate. In that ceremony, the certificate application will be generated and presented in PKCS#10 format[19], and its signature on the information of the public key will be validated.

4.1.2 Authentication of the Identity of a Collective Person

Nothing to remark.

4.1.2.1 MULTICERT Root CA's Self-signed Certificate

MULTICERT stores all documentation used to verify the Certification Authority identity, guaranteeing the verification of identity of its legal representatives, by legally recognised means, and guaranteeing, in the case its legal representatives are not present at the certificate issuing ceremony, sufficient powers of the representative appointed by the entity for such issuance.

The document which supports the issuance of the self-signed certificate of MULTICERT Root CA is a formal document from MULTICERT's Board of Directors, which includes, among others:

a) The Board of Directors' decision to initialize MULTICERT Root CA;
b) Appointment of MULTICERT Root CA's Management Working Group;
c) Information, if necessary, on the identification and powers of the representative(s) appointed by the entity to be present in the issuing ceremony of the self-signed certificate of MULTICERT Root CA.

4.1.3 Authentication of the Identity of a Natural Person

Nothing to remark.

4.1.4 Non-verified Information on the Subscriber/Titleholder

All information described in points 4.1.2 and 4.1.3 is checked.

4.1.5 Validation of Authority

Nothing to remark.

4.1.6 Interoperability Criteria

Nothing to remark.

[19] cf. RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.

4.2 Identification and Authentication for Revocation Request

Given the consequences of revocation of MULTICERT Root CA's self-signed certificate, it is demanded a formal document from MULTICERT's Board of Directors, which includes, among others:

a) The decision of the Board of Directors to revocate MULTICERT Root CA's self-signed certificate;
b) The reasons for the revocation of the certificate;
c) Information, if required, on the identification and powers of the representative(s) appointed by the entity to be present in the revocation ceremony of MULTICERT Root CA's self-signed certificate.

5 Certificate Life-cycle Operational Requirements

5.1 Certificate Application

5.1.1 Who can submit a certificate application

MULTICERT CA's self-signed certificate can only be requested by the Board of Directors of MULTICERT – Serviços de Certificação Electrónica, S.A.

5.1.2 Enrolment Process and Responsibilities

The CA's certificate enrolment process consists of the following steps, to be performed by the relevant Working Groups:

- Generating the key pair (public and private key) in appropriate cryptographic environment;
- Generating the corresponding PKCS#10 in appropriate cryptographic environment.

5.2 Certificate Application Processing

The certificate request is processed as follows:

a) Key pair is generated and the certificate is signed in appropriate cryptographic environment, according to the profile described in this policy;
b) The certificate is made available.

Sections 5.2.1 and **Error! Reference source not found.** describe in detail the whole process.

5.2.1 Performing Identification and Authentication Functions

The relevant Working Groups perform the identification and authentication of all necessary information, according to the established in section 4 of this document.

1. The relevant Working Groups approve the application for the issuance of MULTICERT Root CA's self-signed certificate:
    a. There is express consent of MULTICERT's PKI Management Group.
2. Certificate for Subordinate Certification Authority:
    a. Successful identification and authentication of all necessary information – pursuant to section 4 – all documentation used to verify identity and representation powers is stored;
    b. Valid PKCS#10.

In any other circumstance, the application for issuance of the certificate will be rejected.

After issuing the certificate, the relevant Working Groups provide the certificate to MULTICERT's PKI Management Group and, if appropriate, to the legal representatives of the Subordinate Certification Authority.

5.2.2 Approval or Rejection of Certificate Applications

The approval of a certificate depends on compliance with the requirements demanded in points 5.2 and 5.2.1.
When this does not occur, the issuance of the certificate is rejected.

5.2.3 Time to Process the Certificate Application

After the approval of the certificate application, the certificate shall be issued in no more than ten (10) working days.

5.3 Certificate Issuance

5.3.1 Procedures for issuing a certificate

The issuance of the certificate is done by means of a ceremony that is held within the high security zone of the CE, and where are present:

- The legal representatives of MULTICERT S.A. or the representative(s) named for this ceremony;
- Four (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 key pair 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 pair – This only applies to the generation of the self-signed certificate of MULTICERT Root CA;
- Any observers accepted simultaneously by MULTICERT's PKI Management Group.

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

- Identification and authentication of all the people present in the ceremony, ensuring that the representative(s) and the members of the Working Group have the necessary powers for the acts to be performed;
- The members of the Working Group perform the starting procedure of processing the self-signed certificate of MULTICERT Root CA and issue the certificate (corresponding to the PKCS#10 generated in HSM) in PEM format;
- The issuing ceremony is completed with the execution of the finishing processing procedure for the self-signed certificate, by the members of the Working Group.

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

5.3.2 Subscriber notification as to the issuance of the certificate

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

5.4 Certificate Acceptance

5.4.1 Procedures for Accepting the Certificate

The certificate is considered accepted after the signature of the form of issuance and acceptation of the certificate by the representative(s), according to the issuing ceremony (according to section **Error! Reference source not found.**).

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

a) The subscriber takes notice of the rights and responsibilities;
b) The subscriber takes notice of the functionalities and content of the certificate;
c) The subscriber accepts formally the certificate and its terms of use, signing for that purpose the form for certificate receipt and acceptance.

The necessary procedures in case of expiration, revocation and renewal of the certificate, as well as its terms, conditions and scope of use, are defined in this Certificate Policy and corresponding Certification Practices Statement.

5.4.2 Publication of the Certificate

MULTICERT Root CA doesn't publish the self-signed certificates nor the certificates issued to Subordinate Certification Authorities. They are integrally made available to the subscriber, with the constraints defined in point 5.4.1.

5.4.3 Notification of Certificate Issuance to other Entities

The Accreditation Authority will be notified of the issuance of MULTICERT Root CA's self-signed certificate. The Accreditation Authority will be further invited to the certificate issuing ceremony.

5.5 Key Pair and Certificate Usage

5.5.1 Subscriber Private Key and Certificate Usage

Certificate subscribers 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 points 1.3.1 and 1.3.2 of the Certification Practices Statement (CPS);
c) While the certificate is valid and not in the CRL from MULTICERT Root CA.

5.5.2 Relying Party Public Key and Certificate Usage

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 Certificate Policy and in the related CPS. For this, they should, amongst other, guarantee the fulfilment of the following conditions:

a) Have knowledge and understanding as to 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 of the keys;
e) Trust the certificates, using them whenever they are valid.

5.6 Certificate Renewal with Generation of a New Key Pair

The renewal of certificate keys (*certificate re-key*) is the process in which a subscriber (or sponsor) 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.

The renewal of the certificate with generation of a new key pair is done according to the established in section **Error! Reference source not found.**.

5.6.1 Circumstances for Renewing a Certificate, Generating a New Key Pair

It is considered a valid reason for renewing a certificate, with generation of a new key pair, whenever:

a) The certificate is expiring;
b) The certificate support is expiring;
c) The information on the certificate undergoes changes.

5.6.2 Who may Request Certification of a New Public Key

As in section 5.1.1.

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

As in sections 5.1.2 and 5.2.

5.6.4 Notification of New Certificate Issuance to Subscriber

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

5.6.5 Procedures for Accepting a Renewed Certificate with Generation of a New Key Pair

As in section 5.4.1.

5.6.6 Publication of a Renewed Certificate with Generation of a New Key Pair

As in section 5.4.2.

5.6.7 Notification of Issuance of a Renewed Certificate to Other Entities

As in section 5.4.3.

5.7 Certificate Suspension and Revocation

In practice, certificate revocation and suspension is an action through which the certificate stops being valid prior to the end of its validity period, losing its operability.

Certificates, after being revoked cannot become valid again, whereas suspended certificates may recover their validity.

5.7.1 Circumstances for Suspension

MULTICERT Root CA does not suspend certificates.

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 Circumstances for the Revocation

A certificate may be revoked for one of the following reasons:

- Compromise or suspicion of compromise of the private key;
- Compromise or suspicion of compromise of MULTICERT Root CA's private key;
- Loss of the private key;
- Serious inaccuracies in the data supplied;
- Technological equipment no longer used within MULTICERT Root CA;
- Compromise or suspicion of compromise of the password and access to the private key (example: PIN);
- Loss, destruction or deterioration of the private key support device (example: support/cryptographic token);
- Non-compliance by MULTICERT Root CA or subscriber as to the responsibilities foreseen in this Certificate Policy and/or corresponding CPS;
- Whenever there are credible reasons that infer that the certification services may be compromised in such a way that they place in question the reliability of the certificates;
- By legal or administrative resolution.

5.7.6 Who Can Request Revocation

Having the legitimacy to submit a revocation request, whenever any of the conditions described in point **Error! Reference source not found.** are witnessed, is the following:

a) MULTICERT S.A.'s Board of Directors.

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 of its legal representatives, by a legally recognized mean, not accepting representation powers for the request of self-signed certificate revocation from MULTICERT Root CA.

5.7.7 Procedure for a Revocation Request

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

- All revocation requests shall be addressed to MULTICERT Root CA in writing or through an electronic message, digitally signed by MULTICERT S.A.'s Board of Directors, exposing the reason for the revocation request;
- Identification and authentication of the entity that requests the revocation;
- Registration and archive of the revocation request form;
- Analysis of the revocation request by MULTICERT's PKI Management Working Group, which will provide the revocation information to the other Working Groups;
- 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:

- Date of the revocation request;
- Name of the certificate subscriber;
- Detailed exposure of the reasons for the revocation request;
- Name and functions of the person who requests the revocation;
- Contact information of the person who requests the revocation;
- Signature of the person who requests the revocation.

5.7.8 Revocation Request Grace Period

The revocation will be carried out immediately. After all the procedures are carried out and the validity of the request is verified, the request cannot be cancelled.

5.7.9 Time Period for Processing the Revocation Process

The revocation request should be treated immediately, and therefore, shall never take more than 24 hours.

5.7.10 Revocation Checking Requirement for Relying Parties

Before using a certificate, the relying parties are responsible for verifying the status of all the certificates, through CRL or a verification server as to online status (via OCSP).

5.7.11 Certificate Revocation List (CRL) Issuance Frequency

MULTICERT Root CA makes a new CRL Base available every 4 (four) months.

5.7.12 Maximum Time Period between Issuance and Publishing of the CRL

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

5.7.13 Availability to Verify the Online Status / Revocation of a Certificate

MULTICERT Root CA doesn't provide OCSP validation services for the self-signed certificate.

5.7.14 Requirements for Online Verification of a Revocation

Nothing to remark.

5.7.15 Other Forms Available for Divulging the Revocation

Nothing to remark.

5.7.16 Special Requirements in Case the 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:

- Revocation of the certificate from MULTICERT Root CA and all certificates issued in the trust hierarchy "branch" from MULTICERT Root CA;
- Notification of the Accreditation Authority and all the titleholders of certificates issued in the trust hierarchy "branch" from MULTICERT Root CA;
- Generation of a new key pair for MULTICERT Root CA;
- Renewal of all certificates issued in the trust hierarchy "branch" from MULTICERT Root CA.

6 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 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	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 Certifying Entities.
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 certifying entity 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 a previously enciphered electronic document 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 is recognized, to an entity requesting it and which exercises activity as Certifying Entity, 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.
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 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 reception of an electronic document.

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
CE	Certifying Entity
DCE	Document Certifying Entity
RE	Registration Entity
GMT	Greenwich Mean Time
GNS	*Gabinete Nacional de Segurança* (National Security Office)

MAC	Message Authentication Codes
O	Organisation
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)

7 Approval

Renato Isaias Rodrigues Portela

Assinado de forma digital por Renato Isaias Rodrigues Portela
DN: c=PT, o=MULTICERT - Servicos de Certificacao Electronica S.A., ou=Integracao Desenvolvimento e Consultoria, ou=Certificado para Pessoa Singular, cn=Renato Isaias Rodrigues Portela
Dados: 2014.07.10 09:25:05 +01'00'

[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: 2014.07.10 12:17:28 +01'00'