multicert

Engineering for digital security

Qualified Digital Signature Certificate Policy

Policy

MULTICERT_PJ.CA3_24.1.2_0002_en

Project Identification: PKI MULTICERT

CA Identification: MULTICERT CA

Rating: Public

Version: 3.0

Date: 13/01/2016

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

Document Identification: MULTICERT_PJ.CA3_24.1.2_0002_en

Keywords: Policy, Digital Signature

Document Type: Policy

Title: Qualified Digital Signature Certificate Policy

Original Language: Portuguese

Language of Publication: English

Rating: Public

Date: 13/01/2016

Current Version: 3.0

Project Identification: PKI MULTICERT

CA Identification: MULTICERT CA

Client: MULTICERT S.A.

Version History

Version Nº	Date	Details	Author(s)
1.0	13/01/2009	First Version	MULTICERT S.A.
1.1	23/03/2009	Content Update	MULTICERT S.A.
1.2	24/03/2009	Policies Working Group Revision	MULTICERT S.A.
1.3	25/03/2009	Content Update	MULTICERT S.A.
1.4	25/03/2009	Content Update	MULTICERT S.A.
1.5	25/03/2009	Bibliographic References Update	MULTICERT S.A.
1.6	20/04/2010	Content Revision	MULTICERT S.A.
1.8	05/05/2014	Signature Algorithm Update	MULTICERT S.A.
1.9	09/07/2014	Change in address	MULTICERT S.A.
2.0	10/05/2014	Approved Version	MULTICERT S.A.
2.1	06/11/2015	Content Revision	MULTICERT S.A.
3.0	13/01/2016	Approved Version	MULTICERT S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.CA3_24.1.1_0001_en	Certification Practices Statement	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.2_0001_en	Certificate Policy of MULTICERT Root CA	MULTICERT S.A.
MULTICERT_PJ.CA3_53.2.1_0001_pt	Form of issuance of “specimen” Qualified Digital Signature Certificate.	MULTICERT S.A.

Executive Abstract

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 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.

MULTICERT Certification Authority is duly registered in the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx), with number ANS-ECC-7/2014 on date 20/06/2014, 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 qualified digital signature certificate, which complements and is in accordance with the Certification Practices Statement (CPS) of MULTICERT CA.[1]

[1] *cf.* MULTICERT_PJ.CA3_24.1.1_0001_en.doc. 2009, Certification Practices Statement.

Table of Contents

Qualified Digital Signature Certificate Policy 1
Executive Abstract 3
Table of Contents 4
Introduction 6
Purposes of the document 6
Target Public 6
Document Structure 6
1 Introduction 7
1.1 Overview 7
1.2 Designation and Identification of the Document 7
2 Identification and Authentication 8
2.1 Naming 8
2.1.1 Types of names 8
2.2 Use of the certificate and key pair by the titleholder 9
3 Certificate and CRL Profiles 10
3.1 Certificate Profile 10
3.1.1 Version Number 10
3.1.2 Certificate Extensions 10
3.1.3 Profile of the Qualified Digital Signature Certificate 11
3.1.4 Algorithm OID 19
3.1.5 Name Forms 19
3.1.6 Name Constraints 19
3.1.7 Certificate Policy OID 19
3.1.8 Usage of Policy Constraints Extension 19
3.1.9 Policy Qualifier Syntax and Semantics 19
3.1.10 Processing Semantics for the Certificate Policies critical extension 19
3.2 Specimen Certificate 20
3.3 Certificate Revocation List Profile 20
4 Identification and Authentication 21
4.1 Validating Identity during Initial Registration 21
4.1.1 Method to Prove Possession of Private Key 21
4.1.2 Authentication of the Identity of a Natural Person 21
4.1.3 Non-verified Information on the Subscriber/Titleholder 22
4.1.4 Validation of Authority 22
4.1.5 Interoperability Criteria 22
4.2 Identification and Authentication for Revocation Request 22
5 Certificate Life-cycle Operational Requirements 24
5.1 Certificate Application 24
5.1.1 Who can submit a certificate application 24

5.1.2 Enrolment Process and Responsibilities 24
5.2 Certificate Application Processing 24
5.2.1 Performing Identification and Authentication Functions 24
5.2.2 Approval or rejection of certificate applications 25
5.2.3 Time to process the certificate application 25
5.3 Certificate Issuance 25
5.3.1 Procedures for issuing a certificate 25
5.3.2 Subscriber notification as to the issuance of the certificate 25
5.4 Certificate acceptance 25
5.4.1 Procedures for accepting the certificate 25
5.4.2 Publication of the certificate........ 26
5.4.3 Notification of certificate issuance to other entities 26
5.5 Key pair and certificate usage 26
5.5.1 Subscriber private key and certificate usage........ 26
5.5.2 Relying party public key and certificate usage 26
5.6 Certificate renewal with generation of a new key pair 26
5.6.1 Circumstances for renewing a certificate, generating a new key pair........ 27
5.6.2 Who may request certification of a new public key 27
5.6.3 Processing the certificate renewal request with generation of a new key pair...... 27
5.6.4 Notification of new certificate issuance to subscriber........ 27
5.6.5 Procedures for accepting a renewed certificate with generation of a new key pair. 27
5.6.6 Publication of a renewed certificate with generation of a new key pair........ 27
5.6.7 Notification of issuance of renewed certificate to other entities 27
5.7 Suspension and revocation 27
5.7.1 Circumstances for suspension 28
5.7.2 Who can request the suspension 28
5.7.3 Procedures for a suspension request........ 28
5.7.4 Limited time period for suspension........ 28
5.7.5 Other forms available for divulging the suspension 29
5.7.6 Circumstances for the revocation 29
5.7.7 Who can request revocation........ 29
5.7.8 Procedure for a revocation request 30
5.7.9 Revocation request grace period 30
5.7.10 Time period for processing the revocation request 30
5.7.11 Revocation checking requirements for relying parties 30
5.7.12 Certificate Revocation List (CRL) Issuance Frequency 30
5.7.13 Maximum time period between issuance and publishing of the CRL 30
5.7.14 Availability to verify the online status / revocation of a certificate 30
5.7.15 Requirements for online verification of a revocation 30
5.7.16 Other forms available for divulging the revocation 31
5.7.17 Special requirements in case the private key is compromised 31
6 Audits and safety measures........ 32
Conclusion........ 33
Bibliographic References 34

Introduction

Purposes of the document

The purpose of this document is to define the policies used for the issuance of the qualified digital signature certificate, by MULTICERT CA.

Target Public

This document shall be read by:

- Human resources of MULTICERT CA's Working Groups,
- Third parties auditing MULTICERT CA,
- Public in general.

Document Structure

It is assumed that the reader knows the concepts of cryptography, public key infrastructure and electronic signature. Shall 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 CA[1], being assumed that the reader has read its full content before starting to read this document.

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 Qualified Digital Signature Certificates, issued by MULTICERT CA.

The certificates issued by MULTICERT 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.

1.1 Overview

This CP meets and complements the requirements imposed by the Certification Practices Statement (CPS) of MULTICERT CA[1].

1.2 Designation and Identification of the Document

This document is a Policy for Qualified Digital Signature Certificates. The CP is represented in a certificate by a unique number called “object identifier” (OID). The value of the OID associated with this document is 1.3.6.1.4.1.25070.1.1.1.1.0.1.2.

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

DOCUMENT INFORMATION	
Document Version	Version 3.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Issuing Date	2016 January
Validity	Not applicable
Location	https://pki.multicert.com/index.html

2 Identification and Authentication

2.1 Naming

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

2.1.1 Types of names

The qualified digital signature certificate is identified by a unique name (DN – Distinguished Name), that complies with X.500 standard.

The Distinguished Name of the certificate by MULTICERT CA consists of the following components:

Attribute	Code	Value
Country	C	<Country of nationality of the certificate's titleholder>
Organization	O (optional)	<Organisation to which the certificate's titleholder belongs>
Organization Unit	OU (optional)	<Area/Department of the organisation to which the certificate's titleholder belongs>
Organization Unit	OU	Certificado para pessoa singular – Assinatura Qualificada ou Certificado para pessoa colectiva – Assinatura Qualificada
Common Name	CN	<name of the certificate's titleholder>
Title	title (optional)	<Quality of the certificate's titleholder, in the scope of its use for qualified digital signature>
Surname	SN (optional)	<Surnames of the certificate's titleholder>
GivenName	givenName (optional)	<First names of the certificate's titleholder>
SerialNumber	serialNumber	<unique identifier of the certificate's titleholder>

2.2 Use of the certificate and key pair by the titleholder

The natural person (as identified in *Organization Unit*), identified by a *Distinguished Name,* is the titleholder of the Qualified Digital Signature Certificate. The certificate issued according to this policy corresponds to a qualified digital certificate, as defined by the applicable national laws, being used in any application for purposes of qualified digital signature.

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.[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 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.[2]

The profile of the qualified digital signature certificate is compliant with:

– ITU.T recommendation X.509[3],

– RFC 5280[2], and

– Applicable legislation, national and European.

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 attributes to users or public keys, as well as for managing the certification hierarchy.

[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.

3.1.3 Profile of the Qualified Digital Signature Certificate

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
tbsCertificate	**Version**	4.1.2.1	v3	m	Version certificate in accordance of X.509 Standard
	Serial Number	4.1.2.2	<assigned by the CA to each certificate>	m	
	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"		Holder Country
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		Formal designation of the holder of the organisation
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Other designation of the holder of the organisation
	Common Name (CN)		"MULTICERT - Entidade de Certificação <nnn>"		CA Name
	Validity	4.1.2.5		m	Certificate Validity MUST use UTC time scale until 2049, using *GeneralisedTime* from then on.
	Not Before		<issuing date>		
	Not After		<issuing date + 5 years maximum>		Maximum 5 years of validity.
	Subject	4.1.2.6		m	

[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
	Country (C)		<Country of nationality of the certificate's titleholder>		On scope of Registration Authorities (RA) **OF**[5]**, OM**[6] and **AR**[7], this field assumes the value "PT"
	Organization (O)		<Organisation to which the certificate's titleholder belongs>	o	On scope of RA OF, this field assumes the value "Ordem dos Farmacêuticos". On scope of RA OM, assumes the value "Ordem dos Médicos". On scope of RA AR, assumes the value "Assembleia da República".
	Organization Unit (OU)		<Area/Department of the organisation to which the certificate's titleholder belongs>	o	Not applicable on scope of RA AR
	Organization Unit (OU)		"Certificado para pessoa singular – Assinatura Qualificada" ou "Certificado para pessoa colectiva – Assinatura Qualificada"	o	The qualified digital signatures, issued on scope of the RAs OF and OM, are only for singular person. On scope of RA AR this field is not applicable.
	Common Name (CN)		<name of the certificate's titleholder>		
	Title (title)		<Quality of the certificate's titleholder, in the scope of the use for qualified digital signature> - "Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data", ou informação similar."	o	"Information confirmed by the Certification Authority only at the date of issuance and that was not confirmed after that date", or similar information The quality, on scope of RA OF assumes the value "Farmacêutico" (pharmacist), on scope of RA OM assumes the value "Médico" (Doctor). On scope of RA AR, assumes the quality <Quality of the holder, in the context of the use for qualified signature>.
	Surname (SN)		<surnames of the certificate's titleholder>	o	Not applicable on scope of RA AR

[5] Ordem dos Farmacêuticos
[6] Ordem dos Médicos
[7] Assembleia da República

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	Given Name (givenName)		<first names of the certificate's titleholder>	o	Not applicable on scope of RA AR
	Serial Number (serialNumber)		<unique identifier of the certificate's titleholder>		In general scope, for singular certificate this field assumes the value of the holder NIF, for a certificate issued for collective person, this field assumes the value of NIPC On scope of RAs with restrict scopes, like OF and OM, this field assumes the value "CP <holder identification inside RA>. Not applicable on scope of RA AR.
	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		1.2.840.113549.1.1.1		The rsaEncryption OID identifies RSA public keys.
					pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }
					rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 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.1 type NULL for this algorithm identifier.[8]

	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	

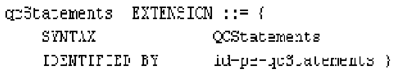
[8] *cf.* RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	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. Gives the type of use of the certificate.
	Digital Signature		“0” selected		
	Non Repudiation		“1” selected		certKeyUsage KeyUsage ::= {nonRepudiation}[9]
	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	4.2.1.4		o	

[9] *cf.* RFC 3739. 2004, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2	m	Identifier of the Policy for Qualified Digital Signature Certificates
	policyQualifier		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html		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 Policy for Qualified Digital Signature Certificates published by the CA. The pointer is in the form of a URI."
	policyQualifier		policyQualiflierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: “O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito.”		OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) “The certificate issued according to this policy is equivalent to a qualified digital certificate, as defined by the applicable national laws.” OID Description: "*User notice* is used to 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)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	o	Certification Practices Statement of MULTICERT CA
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html	o	
			policyQualiflierID: 0.4.0.1456.1.1		Valor do OID: 0.4.0.1456.1.1 (qcp-public-with-sscd)[10] {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd(1)}
	Basic Constraints	4.2.1.9		c	This extension is marked CRITICAL.

[10] ETSI TS 102 853 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies*

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://pki.multicert.com/CA.html	o	
	Freshest CRL	4.2.1.15		o	
	distributionPoint		https://pki.multicert.com/CA.html	o	
	Subject Alternative name	4.2.1.6	RFC822 name = <certificate titleholder’s e-mail address>	o	
	Qualified Certificate Statement	-	id-pe-qcStatements = “1.3.6.1.5.5.7.1.3”[11]  qcStatements EXTENSION ::= { SYNTAX QCStatements IDENTIFIED BY id-pe-qcStatements }		The extension *QCStatements* is an extension introduced by the PKIX Qualified Certificate Profile[9] and ETSI[12].
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Statement from MULTICERT CA, represented by an OID, indicating that this certificate is issued as a qualified certificate, according to Appendix I and II of the EU Directive 1999/93/EC, following the laws of the country where the CA is established.

[11] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html

[12] *cf.* ETSI TS 101 862, 2004-06, Qualified certificate profile, v1.3.2.

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
					The QcEuCompliance (id-etsi-qcs-QcCompliance) statement is associated to a specific identifier which corresponds to OID "0.4.0.1862.1.1". This statement indicates that the certificates are issued in compliance with the ***QCP public*** policy, according to ETSI TS 101 456.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcLimitValue = " 0.4.0.1862.1.2" currency = “EUR” amount = “0” exponent = “1”		Statement through which MULTICERT CA imposes a limit on the value of the transaction for which this certificate can be used, according to the Directive 1999/93/EC and the laws of the country where the CA is established.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcRetentionPeriod = " 0.4.0.1862.1.3" QcEuRetentionPeriod = “20”		This extension contains the indication of the period of retention of information relevant to the issuance and use of the certificate, expressed in number of years after the certificate expiration date.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Statement by MULTICERT CA, indicating that the private key associated to the public key in the certificate is stored in a *Secure Signature Creation Device*, according to appendix III of Directive 1999/93/EC and the laws of the country where the CA is established. This statement indicates that the certificates are issued in compliance with the ***SSCD*** policy, according to ETSI TS 101 456.
	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

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	accessLocation		http://ocsp.multicert.com/ocsp	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)} **Note:** In MULTICERT CA 001 the signature algorithm used was SHA1 (2.16.840.113549.1.1.5). From MULTICERT CA 002 on, it is the mentioned in this document.
	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 (sha-256WithRSAEncryption[13]).

3.1.5 Name Forms

As defined in section **Erro! A origem da referência não foi encontrada.**.

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 CA's Management Working Group.

3.1.7 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).

3.1.8 Usage of Policy Constraints Extension

Nothing to remark.

3.1.9 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.

3.1.10 Processing Semantics for the Certificate Policies critical extension

Nothing to remark.

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

3.2 Specimen Certificate

The Qualified Digital Signature "Specimen" Certificate can be issued every time that is needed to validate the profile, the issuance process and/or its usage. The "specimen" certificate can be issued for testing purposes based on a contract of liability to conclude between MULTICERT and the requiring Entity. This certificate presents the following differences from the usual Qualified Digital Signature Certificates:

- Certificate profile: the prefix "(specimen)" is added to *CommonName* (CN);
- Certificate profile: the attribute serialNumber contains "specimen" followed by a unique sequential number (starting with 0000001);
- Certificate issuance: according to a specific form[14] for internal uses, or by consent of use by the titleholder through a statement of responsibility;

3.3 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[2].

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[2].

The CRL profile conforms to the CRL profile indicated in the Certificate Policy of MULTICERT Root CA.

[14] *cf.* MULTICERT_MO.DOC_53_0142_pt.pdf, Declaração de Responsabilidade sobre a Utilização de Certificados Espécime (*Responsibility Statement on the Use of Specimen Certificates*).

4 Identification and Authentication

4.1 Validating Identity during Initial Registration

For the certificates of qualified digital signature issued in the MULTICERT CA's domain, it is compulsory that the registration is performed in-person, that is, that the validation of the subscriber's identity is done face-to-face (or equivalent method).

4.1.1 Authentication of the Identity of a Natural Person

The process of identity authentication of a natural person ensures that the person to whom the certificate is going to be issued is in fact who he/she declares to be, through the delivery (or request) of the certificate by the titleholder (or legal representative appointed to the request / delivery of the certificate of qualified digital signature, with authenticated signature of the certificate's titleholder) "face-to-face", or by equivalent method.

The "face-to-face" methods or equivalent used are the following:

- In person:
    - Titleholder gets the certificate in MULTICERT S.A. facilities, in one of its offices (Lisbon or Porto) accompanied by an identity document.
    - Through registered mail with hand delivery[15]; the titleholder's identity being verified at the delivery.
- By a third party:
    - The validation of the titleholder's identity is verified, in statement with signature certified and recognized by an entity with legal authority for that act, where the titleholder delegates powers to a third party to get the certificate.

The authenticity of the quality of the certificate's titleholder, in the scope of its use for qualified digital signature, is validated upon submission of evidentiary document issued by an entity which can legally confirm that quality.

Every time that the applicant is not the titleholder, the validation of his/her identity is performed through documents with quality recognition and signature issued by an entity with legal powers for the act.

The authenticity of the quality of the certificate's titleholder, in the scope of its use for qualified digital signature, is validated upon submission of evidentiary document issued by an entity which can legally confirm that quality.

In case of collective person, the certificate will be issued for a natural person to whom representation powers have been assigned by the applicants (legal representatives) of the entity, through document which attests the quality and signature, issued by an entity with legal powers for the act.

Additionally, a validation is made to the email address which will include in certificate. This activity begins after the submission of an application for a qualified digital signature, by sending a request for confirmation e-mail to the titleholder, by MULTICERT, to the address indicated therein.

In this email, the titleholder is asked to confirm the email address by accessing the link provided for that purpose.

[15]http:// http://www.ctt.pt/correio-e-encomendas/enviar-correio/opcoes-de-envio/correio-registado.html

The holder of a Qualified Digital Signature, issued by the MULTICERT CA, cannot activate the certificate if the confirmation e-mail is not made.

4.1.2 Method to Prove Possession of Private Key

In the case of the certificates of qualified digital signature for natural or collective person, the key pair and certificate is supplied in a cryptographic token (SmartCard or USB token), physically personalized for its titleholder. The possession of the private key is guaranteed by the issuing and personalisation process of the cryptographic token, which ensures that:

- The key pair is generated in cryptographic HSM and inserted in the cryptographic token, through secure direct connection and without being recorded in any other device,
- The cryptographic token is personalised for its titleholder,
- Public key is sent to MULTICERT CA for issuing the corresponding digital certificate, which is also archived in the cryptographic token,
- The cryptographic token is delivered to its titleholder face-to-face or by equivalent method (cf. 4.1.2 and 4.1.3).

4.1.3 Non-verified Information on the Subscriber/Titleholder

All information described in points 4.1.2 is checked.

4.1.4 Validation of Authority

Nothing to remark.

4.1.5 Interoperability Criteria

Nothing to remark.

4.2 Identification and Authentication for Revocation Request

Any entity can request the revocation of a certain certificate, when there is knowledge or suspicion of compromise of the titleholder's private key or any other act which recommends this action.

All the MULTICERT RAs store all documentation used to verify the identity and authenticity of the entity which requires the revocation of the certificate of qualified digital signature, which may be, among other:

- The certificate's titleholder (or legal representative appointed to the revocation of the qualified digital signature certificate, recognised through notarisation of the signature of the titleholder), in the case of certificates for natural or collective person;
- Legal representative of the entity that may certify the quality of the certificate's titleholder, affixed in the digital certificate, every time that that quality stops being valid;
- Relying party, every time that it proves that the certificate was used for different purposes from the ones foreseen.

An appropriate form[16] is the base of the request for revocation of the qualified digital signature certificate and contains, among other, the following identification elements from the entity which performs the revocation request:

a) Legal designation;

b) Number of collective person, head office, object, name of the members of corporate bodies and other persons entitled to require it and registration number at the commercial register or/and full name, identity card number or any other element that enables the unequivocal identification of the entity (or its representative) who requests for the revocation;

c) Address and other forms of contact;

d) Request of certificate revoke indicating the distinguished name (DN) attributed to the certificate, as well as its validity period;

e) Reason for revoke a certificate.

The process of identification and authentication for the revocation request of a certificate of natural or collective person is performed through one of the following methods:

- Qualified digital signature of the form,
- Handwritten signature of the form and its delivery by the subscriber in MULTICERT S.A. facilities, namely at the offices in Lisbon or Porto,
- Handwritten signature of the form with notarised recognition of signature,
- Through secure electronic messages, previously defined between MULTICERT RA's and the entity which performs the certificate revocation request.

[16] *cf.* Form to revoke a Qualified Digital Signature, available in - https://www.multicert.com/fotos/editor2/pedido-revogacao-certificado-qualificado.pdf

5 Certificate Life-cycle Operational Requirements

5.1 Certificate Application

5.1.1 Who can submit a certificate application

On a general scope on the RA MULTICERT, which issues certificates for general public, the qualified digital signature certificate for natural person may be subscribed by the certificate holder or legal representative to apply for the effect of request or delivery certificate qualified digital signature, with notarization of the signature of the holder.The qualified digital signature certificate for collective person may be subscribed by the legal representatives of the collective person with powers for the act.

For RAs whose issue is limited to their scope, including the Medical Order (OM), Pharmacists Order (OF) and the Parliament (AR), the certificate request will be signed by the holder in certified quality or function by (s) representative (s) of the legal entity.

5.1.2 Enrolment Process and Responsibilities

The registration process of the request of qualified digital signature certificate is the responsibility of the certificate's titleholder (or legal representative appointed to the act of request/delivery of qualified digital signature certificate, with notarised recognition of the signature of the certificate's titleholder) every time that the request form is filled *online* through the *Web interface* made available by MULTICERT CA.

The registration process of the request of qualified digital signature certificate is the responsibility of MULTICERT CA every time that the request form is sent in manuscript format. However, the accuracy and completeness of the data is always the responsibility of the titleholder (or legal representative appointed to the act of request/delivery of qualified digital signature certificate, with notarised recognition of the signature of the certificate's titleholder).

5.2 Certificate Application Processing

The certificate requests, after being received by RA MULTICERT, are validated if following requirements are fulfilled:

a) Reception and verification of all demanded documentation and authorisations;

b) Verification of the subscriber's identity;

c) Verification of the accuracy and completeness of the certificate request;

d) Request certificate to MULTICERT CA;

Sections 4.1, 5.2.1 and 5.3**Erro! A origem da referência não foi encontrada.**, describe in detail the whole process.

5.2.1 Performing Identification and Authentication Functions

5.2.1.1 Certificate for collective person

As described in section 4.1.2.

5.2.1.2 Certificate for natural person

As described in section 4.1.3.

5.2.2 Approval or rejection of certificate applications

The approval of the 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 five (5) working days.

5.3 Certificate Issuance

5.3.1 Procedures for issuing a certificate

The issuance of the qualified digital signature certificate for collective or natural person is automatically performed by MULTICERT CA's platform, after the registration of the certificate request, being the generation of the key pair performed by the HSM and the certificate issued by MULTICERT CA after the reception of the certificate request (PKCS#10).

As an exceptional measure, whenever a service break occurs on the platform from MULTICERT CA, the key pair will be generated in the card (or USB *token*) with cryptographic chip, being the certificate request (PKCS#10) sent to MULTICERT CA, which will issue it.

5.3.2 Subscriber notification as to the issuance of the certificate

The titleholder of the certificate is considered notified as to the issuance of the certificate when receiving it, according to the "face-to-face" method mentioned in 4.1.3.

5.4 Certificate acceptance

5.4.1 Procedures for accepting the certificate

The certificate is considered accepted after its reception, according to the "face-to-face" method mentioned in 4.1.3.

Note that before the certificate is made available to the subscriber, 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 request.

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 CA doesn't publish the certificates issued; 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

Nothing to remark.

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 1.4.1 and 1.4.2 of the Certification Practices Statement (CPS);

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

In addition, the qualified digital signature certificate aims to be in use in any application for purposes of qualified digital signature.

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 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.

The renewal of the certificate with generation of a new key pair is done according to the established in section 5.3

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 5.3.2.

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

As in section **Erro! A origem da referência não foi encontrada.**.

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 renewed certificate to other entities

As in section 5.4.3.

5.7 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.

More information's in https://www.multicert.com/pt/ajuda/apoio-tecnico/emissao-e-revogacao/suspender-certificado/

5.7.1 Circumstances for suspension

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

- Suspicion of compromise of the private key;
- Suspicion of loss of the private key;
- Suspicion of compromise of the password and access to the private key (example: PIN);
- Suspicion of loss, destruction or deterioration of the private key support device (example: support/cryptographic token);
- Quality of the certificate's titleholder, affixed in the digital certificate, is suspended;
- The powers of representation inscribed in the certificate are suspended or changed;
- 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.

5.7.2 Who can request the suspension

Having the legitimacy to submit a revocation request, whenever any of the conditions described in point 5.7.13 are witnessed, are the following, among other:

a) the certificate titleholder (or legal representative appointed to perform the suspension of the qualified digital signature certificate, with notarised recognition of the signature of the certificate's titleholder), in the case of certificates for natural person and representation of collective person;

b) legal representative of the entity who may confirm the quality of the certificate's titleholder, affixed to the certificate, any time there is suspension of that quality;

c) legal representative of the entity who may appoint the powers of representation of the certificate's titleholder, inscribed in the digital certificate, every time that those powers are suspended or changed;

d) relying party, any time it proves that the certificate was used for purposes different from the foreseen.

MULTICERT CA stores all documentation used to verify the identity and authenticity of the entity which requires the suspension.

5.7.3 Procedures for a suspension request

A webpage available to the titleholder 24*7[17] allows that a qualified digital certificate issued by MULTICERT CA is suspended by the own titleholder immediately, simply by accessing the Internet and knowing the data to be entered.

Apart from this service may be requested suspension through direct contact with MULTICERT (on weekdays from 9 am to 18h) which will provide all the necessary information to carry out suspension of the certificate.

5.7.4 Limited time period for suspension

The suspension is performed immediately by the titleholder.

[17] https://pki.multicert.com/QualCert/SuspensaoCertificadoForm.htm

The request for suspension, after its acceptance by the MULTICERT CA, should be treated immediately, so that under no circumstances will be processed within a period exceeding 24 hours.

The certificate remains suspended for a maximum period of 3 working days. If this period is exceeded, and the revocation isn't requested, the certificate will be active again.

5.7.5 Other forms available for divulging the suspension

The certificate titleholder is notified whenever the certificate is suspended or reactivated.

5.7.6 Circumstances for the revocation

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

- Compromise or suspicion of compromise of the private key ;
- Loss of the private key;
- Serious inaccuracies in the data supplied;
- 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);
- Quality of the certificate's titleholder, affixed in the digital certificate, stops being valid;
- The Representation powers inscribed in the certificate are suspended or changed;
- Non-compliance by MULTICERT CA or titleholder 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;
- Use of certificate for abusive activities;
- Key Compromise risk (for example, due to the weakness of the algorithm or key size);
- Termination of service.

5.7.7 Who can request revocation

Having the legitimacy to submit a revocation request, whenever any of the conditions described in point 5.7.6 are witnessed, are the following, among other (cf. section 4.2**Erro! A origem da referência não foi encontrada.**):

a) certificate titleholder (or legal representative appointed to the revocation of the qualified digital signature certificate, with notarised recognition of the signature of the certificate's titleholder), in the case of certificates for natural or collective person;

b) legal representative of the entity that may certify the quality of the certificate's titleholder, affixed in the digital certificate, every time that that quality stops being valid;

c) legal representative of the entity that may appoint the powers of representation of the certificate's titleholder, affixed in the digital certificate, every time that those powers are suspended or changed;

d) relying party, when it proves that the certificate was used for different purposes from the ones foreseen.

MULTICERT CA stores all information used to verify the identity and authenticity of the entity which requires the revocation.

5.7.8 Procedure for a revocation request

According to section 4.2.

5.7.9 Revocation request grace period

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

5.7.10 Time period for processing the revocation request

The revocation request, after being accepted by MULTICERT CA, shall be treated immediately, and therefore shall never take more than 24 hours.

5.7.11 Revocation checking requirements 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).

5.7.12 Certificate Revocation List (CRL) Issuance Frequency

MULTICERT CA makes a new Base CRL available every week and a new delta-CRL available every day.

5.7.13 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.

5.7.14 Availability to verify the online status / revocation of a certificate

MULTICERT CA has OCSP validation services for the online status of the certificates. That service may be accessed at http://ocsp.multicert.com/ocsp.

The maximum time period between revocation and availability through the OCSP validation service shall not exceed 10 minutes.

5.7.15 Requirements for online verification of a revocation

The relying parties shall have software that can operate the OCSP protocol, in order to obtain the information on the status of the certificate.

5.7.16 Other forms available for divulging the revocation

The certificate titleholder is notified whenever the certificate is revoked.

5.7.17 Special requirements in case the private key is compromised

Only when it refers to compromise of the private key from MULTICERT CA. In case the private key from MULTICERT 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 CA and all the certificates issued in the trust hierarchy “branch” from MULTICERT CA,
- notification of the accreditation authority and all the titleholders of certificates issued in the trust hierarchy “branch” from MULTICERT CA,
- generation of a new key pair for MULTICERT CA,
- renewal of all certificates issued in the trust hierarchy “branch” from MULTICERT CA.

6 Audits and safety measures

All interventions performed in the Certification Authority of MULTICERT are scrutinized by internal auditors. MULTICERT CA is audited by a professional independent from the CE's circle of influence, as demanded by the Accreditation Authority, article 33 of Decree-Law No. 62/2003. Its mission is to audit the infrastructure of the Certification Authority, regarding equipments, human resources, processes, policies and rules, having to submit an annual report, in March, to the Accreditation Authority. The list of Security Auditors from Certifying Entities accredited by the Accreditation Entity is available at http://www.gns.gov.pt/media/6534/listagemdeas.pdf.

The Qualified Digital Certificates issued by MULTICERT CA comply with all technical requirements defined in the following standards:

- CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;
- ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI);
- ETSI TS 101 862 V1.3.3 (2006-01) Qualified Certificate profile;
- ETSI TS 102 042 V2.4.1 (2007-12) Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 102 176-1 v2.0.0 (2007-11) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 280 v1.1.1 (2004-03) X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.

Conclusion

This document defines the certificate policies of the Qualified Digital Signature Certificate used by MULTICERT CA in the support to its activity of digital certification. The hierarchy of trust of MULTICERT Certification Authority:

- Supplies a hierarchy of trust, which will promote the electronic security of the certificates' titleholder, in the relation with third parties,
- Provides the conduction of safe electronic transactions, strong authentication, a means to digitally sign transactions or information and electronic documents, ensuring its authorship, integrity and non-repudiation, and ensuring the confidentiality of the transactions or information.

Bibliographic References

ETSI TS 101 456, 2007-05. Electronic Signatures and Infrastructures (ESI);Policy requirements for certification authorities issuing qualified certificates, v.1.4.3

ETSI TS 101 862, 2006-01. Qualified certificate profile, v1.3.3.

ETSI TS 102 042, 2013-02. Policy requirements for certification authorities issuing public key certificates, v2.4.1.

ETSI TS 102 176-1, 2007-11. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, v2.0.0.

ETSI TS 102 280, 2004-03. X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, v1.1.1.

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

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

RFC 3739. 2004, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Regulation (EU) no. 910/2014 of the European Parliament and of the Council of July 2014 - on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Approval

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

Assinado de forma digital por
[Assinatura Qualificada]
MULTICERT - SERVIÇOS DE
CERTIFICAÇÃO ELECTRÓNICA S.A.
Dados: 2016.02.02 10:17:27
+02'00'