multicert
Engineering for digital security

CIV Certificate Policy

Policy

MULTICERT_PJ.GETGTA_16

Project Identification: PKI MULTICERT

CA Identification: MULTICERT CA

Rating: Public

Version: 1.0

Date: 30/05/2017

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.GETGTA_16

Keywords: Policy, Digital Signature

Document Type: Policy

Title: CIV Certificate Policy

Original Language: Portuguese

Language of Publication: English

Rating: Public

Date: 30/05/2017

Current Version: 1.0

Project Identification: PKI MULTICERT

CA Identification: MULTICERT CA

Client: MULTICERT S.A.

Version History

Version Nº	Date	Details	Author(s)
1.0	30/05/2017	First Version	MULTICERT S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.CA3_24.1.1_0001_en	Certification Practices Statement MULTICERT CA	MULTICERT S.A.
MULTICERT_PJ.ECRAIZ_24.1.2_0001_en	MULTICERT Root CA Certificate Policy	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 subscriber 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 subscriber 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 authenticity, 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, including 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 CIV (*Commercial Identity Verification*) certificates, 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, Certification Practices Statement MULTICERT CA.

Table of Contents

Introduction

Purposes of the document

The purpose of this document is to define the policies used for the issuance of the CIV digital certificates, 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 CIV (*Commercial Identity Verification*) Digital 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 CIV 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 1.3.6.1.4.1.25070.1.1.1.1.0.1.9.

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

DOCUMENT INFORMATION	
Document Version	Version 1.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.9
Issuing Date	2017 June
Validity	1 Year
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 CIV 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 the certificate's subscriber>
Organization	O	<Organisation to which the certificate's subscriber belongs>
Organization Unit	OU	Certificate for Commercial Identity Verification (CIV)
Organization Unit	OU (optional)	<Area/Department of the organisation to which the certificate's subscriber belongs>
Organization Unit	OU (optional)	<Role of the certificate`s subscriber in the organization>
Common Name	CN	<Name of the certificate's subscriber>

2.2 Use of the certificate and key pair by the subscriber

The natural person (as identified in *Organization Unit*), identified by a *Distinguished Name,* is the subscriber of the CIV Certificate. The certificate issued according to this policy is used in any application for purposes of authentication or 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 subscriber (person or system) with which they will use the encipher mechanism or digital signature. The trust is obtained through the use of X.509 v3 digital certificates, which are a data structure that makes the connection between the public key and its subscriber. This connection is stated through the digital signature of each certificate by a trusted CA. The CA may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the subscriber.

A certificate has a limited validity period, indicated in its content and signed by the CA. Since the signature of the certificate and its validity may be independently verified by any 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 CA that signed the certificate, as well as the name of the CA and related information (such as the validity period), then there may be required an additional certificate to obtain a public key from the CA and validate the user's public key. Generally, to validate the public key from a user, there may be needed a network of multiple certificates, including the public key certificate of the user signed by a CA, and one or more additional certificates from CA`s signed by other CA`s.[2]

The profile of the CIV 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 CIV Card Authentication

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	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"		CA Country
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		Formal designation of the subscriber of the organisation
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Other designation of the subscriber 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 + 3 years maximum>		Maximum 3 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 the certificate's subscriber>		
	Organization (O)		<Organisation to which the certificate's subscriber belongs>		
	Organization Unit (OU)		Certificate for Commercial Identity Verification (CIV)		Type of certificate designation.
	Organization Unit (OU)		<Area/Department of the organisation to which the certificate's subscriber belongs>	o	Optional
	Organization Unit (OU)		<Role of the certificate`s subscriber in the organization>	o	Optional
	Common Name (CN)		<name of the certificate's subscriber>		
	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.[5]
	subjectPublicKey		<Public key with modulus n of 2048 bits>		

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

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Subject Key Identifier	4.2.1.2	The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL. Gives the type of use of the certificate.
	Digital Signature		"1" selected		
	Non Repudiation		"0" selected		certKeyUsage KeyUsage ::= {nonRepudiation}[6]
	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		

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

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.9	m	Identifier of the CIV Certificate Policy
	policyQualifier		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "Certificate issued in accordance with the Certificate Policy in https://pki.multicert.com/"		OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) 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 Identifier
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/		
	Subject Alternative Name	4.2.1.6		m	
	Uniform Resource Identifier (URI)		<uuid of card>		This field is filled with the card uuid, which is defined in accordance with RFC 4122
	Basic Constraints	4.2.1.9		c	This extension is marked CRITICAL.
	CA		FALSE		
	Extended Key Usage	4.2.1.12		c	This extension is marked CRITICAL
	KeyPurposeId		CIV Card Authentication		OID: 1.3.6.1.4.1.25070.1.1.1.1.0.2.1
	CRLDistributionPoints	4.2.1.13		o	

Certificate Component		Section in RFC 5280	Value	Type[4]	Comments
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002.crl	o	URL to access CRL
	Freshest CRL	4.2.1.15		o	
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002_delta.crl	o	URL to access delta CRL
	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	URL to access OCSP
	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. 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 Profile of the CIV Authentication

Certificate Component		Section in RFC 5280	Value	Type[7]	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	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"		CA Country
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		Formal designation of the subscriber of the organisation
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Other designation of the subscriber 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 + 3 years maximum>		Maximum 3 years of validity.
	Subject	4.1.2.6		m	

[7] 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[7]	Comments
	Country (C)		<Country of the certificate's subscriber>		
	Organization (O)		<Organisation to which the certificate's subscriber belongs>		
	Organization Unit (OU)		Certificate for Commercial Identity Verification (CIV)		Type of certificate designation.
	Organization Unit (OU)		<Area/Department of the organisation to which the certificate's subscriber belongs>	o	Optional
	Organization Unit (OU)		<Role of the certificate`s subscriber in the organization>	o	Optional
	Common Name (CN)		<name of the certificate's subscriber>		
	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>		

[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[7]	Comments
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Subject Key Identifier	4.2.1.2	The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL. Gives the type of use of the certificate.
	Digital Signature		"1" selected		
	Non Repudiation		"0" 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		

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

Certificate Component		Section in RFC 5280	Value	Type[7]	Comments
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.9	m	Identifier of the CIV Certificate Policy
	policyQualifier		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "Certificate issued in accordance with the Certificate Policy in https://pki.multicert.com/"		OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) 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 Identifier
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/		
	Subject Alternative Name	4.2.1.6		m	
	Uniform Resource Identifier (URI)		<uuid of the cardholder/subscriber>		This field is filled with the cardholder/subscriber uuid, which is defined in accordance with RFC 4122
	Basic Constraints	4.2.1.9		c	This extension is marked CRITICAL.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			This extension is marked CRITICAL
	KeyPurposeId		Any Extended Key Usage		OID: 2.5.29.37.0
	CRLDistributionPoints	4.2.1.13		o	

Certificate Component		Section in RFC 5280	Value	Type[7]	Comments
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002.crl	o	URL to access CRL
	Freshest CRL	4.2.1.15		o	
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002_delta.crl	o	URL to access delta CRL
	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	URL to access OCSP
	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. 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.

3.1.5 Profile of the CIV Digital Signature Certificate

Certificate Component		Section in RFC 5280	Value	Type[10]	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	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"		CA Country
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		Formal designation of the subscriber of the organisation
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Other designation of the subscriber 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 + 3 years maximum>		Maximum 3 years of validity.
	Subject	4.1.2.6		m	

[10] 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[10]	Comments
	Country (C)		<Country of the certificate's subscriber>		
	Organization (O)		<Organisation to which the certificate's subscriber belongs>		
	Organization Unit (OU)		Certificate for Commercial Identity Verification (CIV)		Type of certificate designation.
	Organization Unit (OU)		<Area/Department of the organisation to which the certificate's subscriber belongs>	o	Optional
	Organization Unit (OU)		<Role of the certificate`s subscriber in the organization>	o	Optional
	Common Name (CN)		<name of the certificate's subscriber>		
	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.[11]
	subjectPublicKey		<Public key with modulus n of 2048 bits>		

[11] *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[10]	Comments
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Subject Key Identifier	4.2.1.2	The key Identifier is composed of the 160-bit SHA-1 hash of the value of the *subjectPublicKey* BIT STRING (excluding the tag, length, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL. Gives the type of use of the certificate.
	Digital Signature		"1" selected		
	Non Repudiation		"1" selected		certKeyUsage KeyUsage ::= {nonRepudiation}[12]
	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		

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

Certificate Component		Section in RFC 5280	Value	Type[10]	Comments
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.9	m	Identifier of the CIV Certificate Policy
	policyQualifier		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "Certificate issued in accordance with the Certificate Policy in https://pki.multicert.com/"		OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) 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 Identifier
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/		
	Subject Alternative Name	4.2.1.6		o	
	RFC 822 (e-mail address)		<subscriber e-mail>		
	Basic Constraints	4.2.1.9		c	This extension is marked CRITICAL.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			This extension is marked CRITICAL
	KeyPurposeId		Client Authentication		OID: 1.3.6.1.5.5.7.3.2
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4

Certificate Component		Section in RFC 5280	Value	Type[10]	Comments
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002.crl	o	URL to access CRL
	Freshest CRL	4.2.1.15		o	
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002_delta.crl	o	URL to access delta CRL
	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	URL to access OCSP
	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. 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.

3.1.6 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]).

3.1.7 Name Forms

As defined in section 2.1.

3.1.8 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.

3.1.9 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 ("*policyQualifierID*: 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).

3.1.10 Usage of Policy Constraints Extension

Nothing to remark.

3.1.11 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.

3.1.12 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 CIV "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 CIV 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 revocation: the certificate is revoked immediately after it is no longer necessary for the purpose that was issued.

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.

4 Identification and Authentication

4.1 Validating Identity during Initial Registration

For the CIV certificates 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 authentication of a natural person ensures that the certificate is delivered to his subscriber (or legal representative appointed to the request / delivery of the CIV certificate, with authenticated signature of the certificate's subscriber) by one of the following methods:

- Delivery of the certificate in the RA (Registration Authority) facilities;
- Delivery of the certificate by registered mail.

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

4.1.2 Authentication of the Identity of a Collective Person

The process of authentication of the identity of a collective person starts with the request for the issuance of a CIV digital certificate for a collective person, by completing a proper form and notarized recognition of the signature of the legal representatives empowered to act in name of the collective person.
In the form will be indicated a natural person to receive the certificate of the collective person, being the authentication of that person carried out according to 4.1.1.

4.1.3 Method to Prove Possession of Private Key

In the case of the CIV certificates, the key pair and certificate is supplied in a cryptographic token (SmartCard), physically personalized for its subscriber. 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 subscriber;
- 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 subscriber face-to-face or by equivalent method (cf. 4.1.1 and 4.1.2).

4.1.4 Non-verified Information on the Subscriber/Subscriber

All information described in points 4.1.1 and 4.1.2 are checked.

4.1.5 Validation of Authority

Nothing to remark.

4.1.6 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 subscriber's private key or any other act which recommends this action.

All the MULTICERT RA`s store all documentation used to verify the identity and authenticity of the entity which requires the revocation of the CIV certificate, which may be, among other:

- The certificate's subscriber (or legal representative appointed to the revocation of the CIV certificate, recognised through notarisation of the signature of the subscriber), in the case of certificates for natural or collective person;
- Legal representative of the entity that may certify the quality of the certificate's subscriber, 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 is the base of the request for revocation of the CIV digital certificate and contains, among other, the following identification elements from the entity which performs the revocation request:

a) Legal designation;
b) Name of the certificate holder;
c) Number of collective person, name of the members of corporate bodies and other persons entitled to require it and its signatures according to the identification document;
d) Request of certificate revoke indicating the reference of the certificate;
e) Reason for revoke a certificate.

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

- Handwritten signature of the form and its delivery by the subscriber and the person(s) responsible for the company in GET Group RA`s facilities;
- Through secure electronic messages, previously defined between GET Group RA's and the entity which performs the certificate revocation request.

5 Certificate Life-cycle Operational Requirements

5.1 Certificate Application

5.1.1 Who can submit a certificate application

The certificate request may be subscribed by the legal representatives of the collective person with powers for the act.

5.1.2 Enrolment Process and Responsibilities

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

5.2 Certificate Application Processing

The certificate requests, after being received by RA GET Group RA, 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 legal representatives of the collective person identities;
d) Verification of the accuracy and completeness of the certificate request;
e) Request certificate to GET Group RA.

Sections 4.1, 5.2.1 and 5.3, 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 4.1.4.

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 CIV digital certificate 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 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 subscriber 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 4.1.4.

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.
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 CA.

In addition, the CIV digital certificate aims to be in use in any application for purposes of authentication and/or 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:

f) The certificate is expiring;

g) The certificate support is expiring;

h) 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.

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 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/en/client-support/digital-certificates/revocation/.

5.7.1 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 (cryptographic smartcard);
- Quality of the certificate's subscriber, affixed in the digital certificate, stops being valid;
- The Representation powers inscribed in the certificate are suspended or changed;
- Non-compliance by GET Group RA, MULTICERT 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;
- Use of certificate for abusive activities;
- Key Compromise risk (for example, due to the weakness of the algorithm or key size);
- Termination of service.

5.7.2 Who can request revocation

Having the legitimacy to submit a revocation request, whenever any of the conditions described in point 5.7.1 are witnessed, are the following, among other (cf. section 4.2):

a) certificate subscriber (or legal representative appointed to the revocation of the CIV digital certificate, with notarised recognition of the signature of the certificate's subscriber);

b) legal representative of the entity that may certify the quality of the certificate's subscriber, 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 subscriber, 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.

GET Group RA stores all information used to verify the identity and authenticity of the entity which requires the revocation.

5.7.3 Procedure for a revocation request

According to section 4.2.

5.7.4 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.

5.7.5 Time period for processing the revocation request

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

5.7.6 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).

5.7.7 Certificate Revocation List (CRL) Issuance Frequency

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

5.7.8 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.

5.7.9 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.

5.7.10 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.

5.7.11 Other forms available for divulging the revocation

The certificate subscriber is notified whenever the certificate is revoked.

5.7.12 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 subscribers 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.

Conclusion

This document defines the certificate policies of the CIV Digital 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' subscriber, 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

- 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.
- 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 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- Certificate Practices Statement MULTICERT CA (MULTICERT_PJ.CA3_24.1.1_0001_en).
- FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors.
- NIST SP 800-73-4 Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation.
- RFC 4122. 2005, A Universally Unique Identifier (UUID) URN Namespace.