multicert
Engineering for digital security

Certification Practices Statement MULTICERT CA

Policies

MULTICERT_PJ.CA3_24.1.1_0001_en

Project Identification: MULTICERT PKI's PKI

CA Identification: MULTICERT CA

Rating: Public

Version: 5.0

Date: 02/08/2017

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

Document Identifier: MULTICERT_PJ.CA3_24.1.1_0001_en

Key Words: MULTICERT CA, EC MULTICERT, Declaração de Práticas de Certificação

Document Type: Policy

Title: Certification Practices Statement

Original Language: Português

Language of Publication: English

Rating: Public

Date: 02/08/2017

Current Version: 5.0

Projet Identification: MULTICERT PKI

CA Identification: MULTICERT CA

Client: MULTICERT S.A.

Version History

Version Nr.	Date	Details	Author(s)
1.0	28/12/2008	First Version	Multicert
1.3	20/04/2010	Content Revision	Multicert
2.0	21/05/2014	Update with renewal of Multicert CA	Multicert
2.1	22/02/2015	Content Revision	Multicert
3.0	20/01/2016	Versão Aprovada	Multicert
3.1	28/03/2016	Inclusion Link to General Conditions Update suspension link Updtae version of CABForum Baseline requirements	Multicert
4.0	30/03/2016	Approved Version	Multicert
4.1	26/04/2016	Revision	Multicert
4.2	22/02/2017	Revision according with ETSI EN 319 411-1	Multicert
4.3	29/05/2017	Electronic Seal Inclusion	Multicert
5.0	31/05/2017	Approved Version	Multicert

Related Documents

Document ID	Details	Author(s)
Multicert_PJ.CA3_24.1.2_0001_en	Certificate Policy of Multicert Root CA	Multicert
Multicert_PJ.CA3_24.1.2_0002_en	Qualified Digital Signature and Electronic Seal Certificate Policy	Multicert
Multicert_PJ.CA3_24.1.2_0003_en	Authentication Certificate Policy	Multicert
Multicert_PJ.CA3_24.1.2_0009_en	Web Server Certificate Policy	Multicert

Executive Summary

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

The infrastructure of Multicert CA provides a hierarchy of trust which promotes the electronic security of the titleholder of the digital certificate. Multicert CA establishes a structure of electronic trust, which enables carrying out secure electronic transactions, strong authentication, a means of electronically signing transactions or electronic information and documents, assuring their authorship, integrity, and non-repudiation, as well as the confidentiality of the transactions or information.

Multicert Certification Authority is duly registered in the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx), with credencial number ANS-ECC-7/2014 in 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 procedures and practices in use by Multicert CA for supporting its activity of digital certification, being referred to as the Certification Practices Statement by the Certification Authority Multicert.

Table of Contents

Introduction

Purposes

The purpose of this document is to define the procedures and practices used by Multicert Certification Authority (Multicert CA) for supporting its activity of digital certification.

Target Public

This document shall be read by:

- Human resources named for the Multicert CA's Working Groups,
- Third parties responsible for auditing Multicert CA,
- All people, in general.

Document Structure

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

This document follows the structure defined and proposed by the PKIX working group (*Public-Key Infrastructure X.509*) from IETF (*Internet Engineering Task Force*), in document RFC 3647[1].

The first seven chapters are dedicated to describing the most important procedures and practices in the scope of the digital certification by Multicert CA. Chapter eight describes compliance audits and other assessments. Chapter nine describes legal subjects.

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

1 Introduction

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

This document describes the general practices for the issuing and management of the certificates, followed by the Certification Authority Multicert (Multicert CA), and explains the meaning and function of a certificate, as well as the procedures that shall be followed by Trusting Parties, and by any other interested person, in order to trust in the certificates issued by Multicert CA. This document may undergo regular updates.

The certificates issued by Multicert CA hold a reference to the CPS allowing the trusting parties and other interested persons to find information about the certificate and the entity that issued it.

Multicert Certification Authority is owned by the company Multicert – Serviços de Certificação Electrónica, S.A.

1.1 Overview

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

This document applies specifically to Multicert CA, acknowledges and implements the standards identified on section "Bibliographic References".

1.2 Designation and Identification of the Document

This document is the Certification Practices Statement of Multicert CA. The CPS is represented in a certificate by a unique number called "object identifier" (OID). The OID of the Certificate Policy is used according to the information described in section 3.1.1.

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

DOCUMENT INFORMATION	
Document Version	Version 5.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.1.0.7
Issuing Date	August 2017
Validity	1 year
Location	https://pki.multicert.com/index.html

1.3 Participants in the Public Key Infrastructure

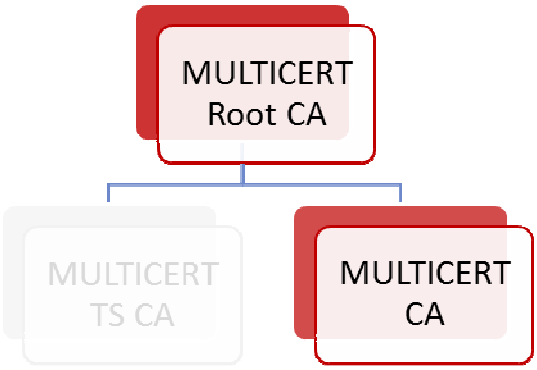
1.3.1 Certification Authorities

Multicert CA is a certifying entity accredited by the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx), as provided by European and Portuguese laws, and is therefore legally capable of issuing all types of digital certificates, including qualified digital certificates (digital certificates with the highest degree of security provided by law). It falls within two hierarchies of trust:

- Multicert Root CA, duly registered in the National Security Authority;
- *Baltimore CyberTrust Root* accredited by *WebTrust* (http://www.webtrust.org/) and present in most operating systems and web browsers.

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

Schematically:



[2]

Multicert CA issues certificates:

- Qualified Certificates[3]:
  - for digital signature:
    - Individual
      - Particular – Certificate which includes the name of its titleholder, which will be used to sign documents.
      - Professional – Certificate with the same characteristics of the particular, although is always relative to a legal entity, like a Medician or an enginner.
      -
      - Representation Purposes – Like the Particular, this Certificate includes the name of a Legal Entity, the name of who represents it and the identification of the representation powers (powers inherent to the position or by proxy delegation of powers), relevant for the signature of documents.
- For Electrónic Seal – Certificate issued to an Organization. The certificate holder is a legal person. This certificate can be used, for example, for signing electronic invoices (issuing large

[2] Multicert CA – Multicert Certification Authority also referred to in this document as Multicert CA - Certification Authoritie of Multicert
[3] According to ETSI 101456 (5.3.1 - QCP public + SSCD)

volumes with increased security), electronic account statements, electronic statements, certificates and other types of online documents issued by public authorities.

- Advanced Certificates[4]:
  - Certificates issued for individuals and professionals, allowing the electronic signature of documents (without provative value) and the safe univocal electronic identification of a person.
- SSL Certificates
  - Digital certificate aimed at ensuring the authenticity of a website, the ownership of a domain or the confidentiality of the information transacted.
- Certificates for services of Multicert CA, i.e., certificates for the required services under the scope of Multicert CA:
  - OCSP online validation

Multicert CA Certificate Information:

CERTIFICATE INFORMATION	
Distinct Name	CN=Multicert Entidade de Certificação 001, OU = Entidade de Certificação Credenciada, O = Multicert - Serviços de Certificação Electrónica S.A.,C = PT
Validity	29/05/2020
Thumbprint	ef 2e 98 f4 42 ee cd 10 b9 8f 2a da 72 16 09 8c e4 83 53 18
Issuing	CN = Baltimore CyberTrust Root,OU = CyberTrust,O = Baltimore,C = IE

CERTIFICATE INFORMATION	
Distinct Name	CN=Multicert Certification Authority 002, OU = Accreditted Certification Authority, O = Multicert - Serviços de Certificação Electrónica S.A.,C = PT
Validity	13/05/2025
Thumbprint	92 4f d9 c5 00 21 5f a0 24 d4 21 57 86 e2 d2 ac 19 81 21 ed
Issuing	CN = Baltimore CyberTrust Root,OU = CyberTrust,O = Baltimore,C = IE

CERTIFICATE INFORMATION	
Distinct Name	CN=Multicert Certification Authority 002, OU = Accreditted Certification Authority, O = Multicert - Serviços de Certificação Electrónica S.A.,C = PT
Validity	19/09/2025
Thumbprint	d5 c7 ec 2e 03 f5 ce a7 b6 3a 3b b4 89 75 92 77 6a 6b f8 d6
Issuing	CN = Multicert Root Certification Authority 01,O = Multicert - Serviços de Certificação Electrónica S.A.,C = PT

[4] According to ETSI 102 042 (NCP)

1.3.2 Registration Authorities

Register Authoritie (RA) is the entity that approves the distinguished names (DN) of the holders of certificates and through evaluation of the application, accepts or rejects the request of it. In addition, the RA also has authority to approve the revocation or suspension of certificates.

The following RA's belong to Multicert PKI :

- Internal RA - Operationalized by the internal services of Multicert, which holds the CA:
  - Multicert RA (RA MC)
- External RA - Operationalized by entities outside Multicert, requesting qualified digital certificates to Multicert CA:
  - Parlement (RA AR);
  - Pharmacists Order (RA OF);
  - Doctors Order (RA OM).

The Multicert Registration Authorities meet the requirements set forth herein and are subject to external audits, conducted by the National Security Office, and Internal Audits carried out by the Multicert CA.

The issue of digital certificates attached the following terms and conditions of the Digital Certificate Issuance Agreement:

- ER MC, ER OM e ER OF:
  - https://pki.multicert.com/politicas/contrato/cgerais.html.
- ER AR:
  - http://app.parlamento.pt/ERAR/Condicoes_Gerais_ERAR_v1.0.pdf.

1.3.2.1 Internal RA

Under the Multicert PKI, the entity is materialized by the registration of the same internal services which register and validating the necessary data, as explained in the Certificate Policy of each type of certificates issued.

1.3.2.2 External RA

The Multicert PKI descentralizes, considering qualified signatures, this function through external RAs, that carry out the following activities:

- Certificate request validation,
- Once approved, the issue of the certificate request submission to the Multicert CA,
- The CA returns the certificate, which is customized in secure device,
- The RA has responsibility for ensuring the delivery of the certificate to the holder thereof, or who legally represents it.

In addition to these activities, these RA's can also request to the Multicert CA certificate revocation, so that the holder thereof cease to serve on the scope for which it was issued.

Note that the Registry Entities associated with Multicert are typically organizations that make certificates available in a controlled environment and only to their signatories. Qualified Certificates issued under the Multicert Registration Authorities are only for Digital Signature.

1.3.3 Certificate titleholders

Within the context of this document, the term subscriber/titleholder applies to all final users to whom were attributed certificates by Multicert CA.

Titleholders of certificates issued by Multicert CA are considered those whose name is inscribed in the field "*Subject"* of the certificate and use the certificate and corresponding private key according to the established in the different certificate policies described in this document; certificates being issued for the following holders' categories:

- Natural person or entity;
- Organisations, or
- Services (such as computers, *firewall*, *routers*, servers, etc.).

In some cases, the certificates are directly issued to natural person or entity for personal use. However, there are cases in which the person requiring the certificate is different from its titleholder, for example, an organisation can request certificates for its employees, so that they can represent the organisation in transactions/electronic commerce. In these situations the entity which requires the issuance of certificate is different from its titleholder.

1.3.3.1 Sponsor

The issuance of certificates for technological equipments is always carried out under human responsibility, with this entity being designated as sponsor.
The sponsor accepts the certificate and is responsible for its correct use, as well as for the protection and safeguarding of its private key.

1.3.4 Trusting Parties

Trusting or recipient parties are natural persons, entities or equipment that trust the validity of the mechanisms and procedures used in the association process of the titleholder's name with its public key, that is, they trust that the certificate corresponds in reality to whomever it says it belongs to.

In this document, a trusting party is considered that which trusts the content, validity and applicability of the certificate issued by Multicert CA.

1.3.5 Other participants

1.3.5.1 Supervisory Body

The Supervisory Body is the competent entity for the accreditation and supervision of the Certifying Entities.

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

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

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

b) Registry: procedure without which the CA can't issue the Qualified Certificates;

c) Supervision: procedure based on the inspections made to the CA to regularly check the compliance parameters;

1.3.5.2 Registration Authorities

As described in 1.3.2

1.3.5.3 External entities to provide services

Entities providing services support to CA Multicert have their responsibilities defined properly through contracts established with them.

1.3.5.4 OCSP Validity Entity

The OCSP Validation Entities have the function of checking the status of the issued certificates, by using the *Online Certificate Status Protocol*[5] (OCSP), in order to determine the current status of the certificate, required by an entity, without having to check the status by consulting the Certificate Revocation List (CRL).

The OCSP Validation Entity service is provided by Multicert CA.

1.3.5.5 Security Auditor

Independent from the CA circle of influence, this figure acredited by the Acreditantio Nacional Body. Its mission is to audit the CA infrastructure regarding the equipments, human resources, processes, policies and rules in order to evaluate the compliance of trust services with the Regulation 910/2014.**Error! Hyperlink reference not valid.**
Multicert PKI is audited by a Conformity Assessment Body (duly registered with the National Accreditation Body), which issues a Compliance Audit Report (CAR) to be made available to the Supervisory Entity in ordedr to evaluate the continuity of the provision of the trust services.

Compliance audits shall be carried out at least every 12 months in order to confirm that Multicert, as being a qualified provider of reliable services and the reliable services it provides, complies with the requirements established by the Regulation 910/2014.

1.4 Certificate Use

The certificates issued in the Multicert CA domain are used by the diferente holders, systems, applications, mechanisms and protocols with the purpose of ensuring the following security services:

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

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

[5] *cf.* RFC 2560. 1999, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

1.4.1 Appropriate Use

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

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

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

1.4.1.1 Certificates issued for natural person or entity

The certificates issued for natural persons or entities, according to the type of certificate acquired, can be used for:

- signing documents
- signing electronic mail

1.4.1.2 Certificates issued for organisations

The certificates for organisations are issued to ensure the site domain property and/or identification of the organisation.

1.4.2 Non-Authorised Use

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

The certificates issued by Multicert CA cannot be used for any other purpose outside the scope of the uses previously described.

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

1.5 Policy Management

1.5.1 Entity responsible for document management

The management of this certificate policy is the responsibility of the Authentication Group of the Multicert CA.

1.5.2 Contact

NAME	Authentication Group of the Multicert CA

Manager:	Sara Loja
Address:	Multicert S.A. Lagoas Park Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras, Portugal
E-mail:	pki.documentacao@multicert.com
Webpage:	www.multicert.com
Telephone number:	+351 217 123 010

1.5.3 Entity responsible for determining the compliance of the CPS regarding the Policy

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

1.5.4 Procedures for Approving the CPS

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

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

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

1.6 Definitions and acronyms

1.6.1 Definitions

Iten	Definition
Digital signature	Advanced electronic signature modality based on an asymmetric cryptographic system made up by an algorithm or series of algorithms, with which is generated an exclusive and interdependent asymmetric key pair, one of which is private and another public, and which allows the titleholder to use the private key to declare authorship of the electronic document to which the signature has been added and agreement with its

	content, and the recipient to use the public key to check if the signature was created with the corresponding private key and if the electronic document was changed after the signature was added.
Electronic signature	Is the result of electronic processing of data, susceptible of constituting the object of individual and exclusive right and used to make the authorship of the electronic document known.
Advanced electronic signature	Electronic signature that fulfils the following requirements: i) Identifies unequivocally the titleholder as author of the document; ii) Its addition on the document depends only on the will of the titleholder; iii) Created with means which the titleholder can maintain under its exclusive control; iv) Its connection with the document enables detecting all and any change resulting from its content.
Qualified electronic signature	Digital signature or other advanced electronic signature modality that satisfies safety demands identical to those of digital signatures based on a qualified certificate and created through a secure device for signature creation.
Accreditation Authority	Competent entity for the accreditation and supervision of the Certifying Entities.
Certificate	Electronic document which connects the data for verifying the signature of its titleholder and confirms the titleholder's identity.
Certificate for website authentication	Certificate that allows the authentication of a website and associate it with the natural or legal person for whom the certificate has been issued.
Advanced Certificate	Certificate which offers the same quality of a qualified certificate, however without the implicit legal constraints of the qualified signature and without requiring the use of a safe device for its creation. It doesn´t confer the legal probative value of a qualified signature.
Qualified Certificate for website authentication	Qualified Certificate that allows the authentication of a website and associate it with the natural or legal person for whom the certificate has been issued and is compliant with the Regulation (EU) N° 910/2014.
Qualified Certificate	Certificate issued by a trust service provider and meets the requirements defined in the regulation 910/2014.

Normalized Certificate	The same as Advanced Certificate
Private Key	Element of asymmetric key pair meant to be known only by its titleholder, through which the digital signature is added on the electronic document or a previously enciphered electronic document with the corresponding public key is deciphered.
Public Key	Element of asymmetric key pair meant to be released, with which the digital signature added on the electronic document by the titleholder of the asymmetric key pair is verified or by which an electronic document to be transmitted to the titleholder of the same key pair is enciphered.
Accreditation	Act by which is recognized, to an entity requesting it and which exercises activity as Certifying Entity, the fulfilment of the requirements defined in the present diploma for the purposes therewith foreseen.
Data for creating a signature	Unique set of data, such as private keys, used by the titleholder to create an electronic signature.
Data for verifying a signature	Set of data, such as public keys, used to verify an electronic signature.
Device for signature creation	Software or equipment device used to make the treatment of data for signature creation possible.
Safe device for signature creation	Device for creation of signatures which ensures, through appropriate technical and procedural means, that: i) Data necessary to create a signature, used in generating a signature, can only occur one time and that confidentiality of that data is assured; ii) Data necessary to create a signature, used to generate a signature, cannot, with a reasonable degree of safety, be deduced from other data and that the signature is protected against falsifications carried out through the technologies available; iii) Data necessary to create a signature, used to generate a signature, may be effectively protected by the titleholder against the illegitimate use by third parties; iv) Data that require a signature are not modified and may be presented to the titleholder before the signature process.
Electronic document	Document elaborated through data electronic processing.
E-mail	Identification of the appropriate computer equipment to receive and

	store electronic documents.
Certifying Entity	Entity or natural or collective person who creates or provides means to the creation and verification of signatures, issues the certificates, ensures advertising and provide other services related with electronic signatures.
Certification Body	Public or private entity qualified to assess and certify the conformity of processes, systems and electronic signature products with the requirements refered in paragraph c), no. 1, article 12 from Decree-Law 62/2003.
Electronic Signature Product	Software, equipment device or its specific components, meant to be used for the provision of qualified electronic signature services by a certifying entity or for the creation and verification of qualified electronic signature.
Electronic Seal	Data in electronic format logically associated with other data in electronic format to guarantee its origin and integrity.
Advanced Electronic Seal	An electronic seal that meets the requirements of the article 36 from the Regulation 910/2014.
Qualified Electronic Seal	An electronic seal created by a qualified secure cryptographic device that meets the requirements of the Regulation 910/2014.
Titleholder	Natural or collective person identified in a certificate as the holder of a signature creation device.
Chronological validation	Statement of an EC attesting the date and time for creation, expedition or reception of an electronic document.

1.6.2 Acronyms

Acronym	
ANSI	American National Standards Institute
CA	Certification Authority
CRL	Certificate Revocation List

DL	Decree-Law
DN	Distinguished Name
CPS	Certification Practices Statement
EAL	Evaluation Assurance Level
MAC	Message Authentication Codes
NCP	Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SGCVC	System for Managing the Certificate Life Cycle
SSCD	Secure Signature-Creation Device

1.6.3 Bibliographic References

CA/Browser Forum – Baseline Requirements, v1.3.3;

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 (2013-02) *Policy requirements for certification authorities issuing public key certificates*;

ETSI TS 102 176-1 v2.1.1 (2011-07) *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;*

Decree-Law no. 290-D/99, from August 2nd.

Decree-Law no. 62/2003, from April 3th.

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

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

FIPS 140-2. 1994, *Security Requirements for Cryptographic Modules*.

ISO/IEC 3166. 1997, *Codes for the representation of names and countries and their subdivisions*.

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

NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm* (SHA-1). *National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce*.

RFC 1421. 1993, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.*

RFC 1422. 1993, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.*

RFC 1423. 1993, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.*

RFC 1424. 1993, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.*

RFC 2560. 1999, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification, version* 1.7.

RFC 3161. 2001, *Internet* X.509 *Public Key Infrastructure Time-Stamp Protocol* (TSP).

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

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

RFC 4510. 2006, *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

RFC 4210. 2005, *Internet X.509 Public Key Infrastructure Certificate Management Protocol* (CMP).

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

2 Publishing and Storage Responsibility

2.1 Repositories

Multicert S.A. is responsible for the repository functions of the CE Multicert, publishing, among others, information related to the practices adopted and the status of the issued certificates (CRL).

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

- 99,5% platform service availability, 24hx7d, excluding required maintenance performed in time of less use, assuring during the available time:
  - Minimum 99,990% of answers to requests for obtaining the CRL;
  - Minimum 99,990% of answers to requests for the CPS document;
- Maximum number of requests for CRL: 50 requests/minute;
- Maximum number of requests for CPS: 50 requests/minute;
- Medium number of requests for CRL: 20 requests/minute;
- Medium number of requests for CPS: 20 requests/minute.

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

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

2.2 Publishing of Certification Information

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

Multicert always makes the following public information available *online*:

- Electronic copy of the most recent version of this CPS and Certificate Policy (CP) from Multicert CA, electronically signed by a duly authorised individual and with a digital certificate attributed for that purpose:
  - CPS from Multicert CA made avilable in URI: https://pki.multicert.com/index.html,
  - *on-line* OCSP validation certificate Policy made available in URI: http:// https://pki.multicert.com/index.html,
  - Authentication certificate Policy made available in URI: https://pki.multicert.com/index.html,
  - Qualified digital signature e electronic seal certificate Policy made available in URI: https://pki.multicert.com/index.html.
  - WebServer Certificate Policy made available in URI: http://pki.multicert.com/index.html.

- CRL from Multicert CAs
  - MULITCERT CA 001
    - CRL URI: http://ec2pki.multicert.com/crl/crl_<ID_CA>.crl
      - Delta-CRL URI: https://pki.multicert.com/crl/crl_mca001_delta.crl
  - MULITCERT CA 002
    - CRL URI: http://ec2pki.multicert.com/crl/crl_mca002.crl
      - Delta-CRL URI: http://ec2pki.multicert.com/crl/crl_mca002_delta.crl
- Certificate from Multicert CA
  - Multicert CA 001 - URI: https://pki.multicert.com/cert/Multicert_CA/mca_001.cer
  - Multicert CA 002 – URI: http://ec2pki.multicert.com/cert/mca_002.cer
- Other relevant information – URI: https://pki.multicert.com.

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

Compliance Statements will always available whenever requested through the email pki.documentacao@multicert.com.

Multicert CA complies with the current version of the baseline requirements for the Issuance and Management of *Publicly-Trusted* Certificates, published by **CA/*Browser Forum*** in the document "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*", available at http://www.cabforum.org. In case there is any inconsistency between this document and the described in the *Baselines* document, the information in the document issued by the CA/*Browser Forum* overlaps what is described in this document.

2.3 Periodicity of the publication

The updates to this CPS and corresponding CPs, performed yearly, shall be published immediately after its approval by the Management Group, according to section 9.12.

The certificate from Multicert CA shall be published immediately after its issuing. The CRL from Multicert CA shall be published at least once a week. Delta-CRL from Multicert CA shall be published, at least, every day.

2.4 Access control to the repositories

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The naming follows the following convention:

- to certificates of a natural person is given the real titleholder's name (or pseudonym),
- to certificates of a collective person is given the entity's name, being referred in the certificate the name of the legal representative;
- to certificates of services is given the qualified name of domain and/or the scope of its usage.

3.1.1 Types of names

The certificate by Multicert CA as well as the certificates issued by Multicert CA are identified by a unique name (DN – Distinguished Name) that complies with X.500 standard.

The Distinguished Name of these certificates is identified in the respective Certificate Policies:

Type of Certificate	OID of the Certificate Policy
Multicert CA (self-signed root)	1.3.6.1.4.1.25070.1.1.1.1.0.1.1
OCSP online validation	1.3.6.1.4.1.25070.1.1.1.0.1.3
Qualified Digital Signature and Electronic Seal	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Authentication	1.3.6.1.4.1.25070.1.1.1.1.0.1.3
Advanced Certificates	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Web Server Certificate (OV[6])	1.3.6.1.4.1.25070.1.1.1.1.0.1.5
Application	1.3.6.1.4.1.25070.1.1.1.1.0.1.6
Virtual TPA	1.3.6.1.4.1.25070.1.1.1.1.0.1.8

3.1.2 Need for significant names

Multicert CA shall ensure, inside its trust infrastructure:

- the non existence of certificates that, having the same DN may identify distinct entities,
- the relation between the titleholder and the organisation to which he/she belongs is the same which is referred in the certificate and is easily noticeable and identifiable by humans (except the certificates with pseudonyms).

[6] Organizational Validation

3.1.3 Titleholders' anonymity or pseudonym

Multicert CA issues certificates with pseudonym of titleholders, assuring that,

- the certificate contains the titleholder's pseudonym, clearly identified as such, and the elements which testify the true identity of the applicants holding a certificate with pseudonym are conserved,
- it will communicate to the judicial authority, whenever it is required in the terms foreseen by law, the data related to the identity of the titleholders of certificates issued with pseudonym, following, in the applicable, the provisions of article no. 182 of the Code of Criminal Procedure.

3.1.4 Interpretation of the names formats

The rules used by Multicert CA for the interpretation of the names formats follow the established in RFC 5280[7], assuring that all *DirectoryString* attributes of the *issuer* and *subject* fields of the certificate are coded in a *UTF8String*, except the attributes *country* and *serialnumber*, which are coded in a *PrintableString*.

3.1.5 Name uniqueness

Identificators of type DN are unique for each certificate titleholder, issued within Multicert CA, and it is not ambiguous.

According with its issuing procedures, Multicert CA rejects the issuance of certificates with the same DN to distinct titleholders. For each type of issued certificate, the corresponding Certificate Policy indicates the s*erialnumber* content, which shall be selected in order to assure the uniqueness of the field and not induce a trusting party in ambiguity.

3.1.6 Registered trademark recognition, authentication, and role

The entities which require a certificate have to show that they have the right to use the required name, as the designations used in the certificates issued by Multicert CA cannot infringe the intellectual property rights of other individuals or entities.

For the procedure of authentication and identification of the certificate's titleholder, previous to its issuance, the entity which requires the certificate has to present legal documents that prove the right to use the name required.

3.2 Validation of identity in the initial registration

3.2.1 Qualified Certificate

3.2.1.1 Electronic Signature (eSign)

According to Qualified Electronic Signature and Electronic Seals Certificate Policy, section 4.1.1, available in http://pki.multicert.com/CA.html.

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

3.2.1.2 Selo Eletrónico (eSeal)

According to Qualified Electronic Signature and Electronic Seals Certificate Policy, section 4.1.1, available in http://pki.multicert.com/CA.html.

3.2.1.3 Webserver Certificate – Organization Validation (OV)

Certificates for web site authentication are issued once the legal existence of the same is guaranteed and that other attributes to include in the certificate are real, for example domain ownership.

The validation of the applicants for these certificates is done through supporting documents, issued by credible entities that allow the verification of data of the organization requesting the certificate, as well as of its legal representatives (eg permanent certificate).

When a domain name or email address is included in the certificate, Multicert authenticates the Organization's right of use to use the domain name as a fully qualified domain name (Certificate Policy SSL, available at https://pki.multicert.com/pol/cp/).

The confirmation of the certificate request is made through a call, recorded, made to the number provided by a credible source (official website, whois, etc) and confirmed the information with the technical responsible for the certificate request.

3.2.1.4 Services Certificate

The issuance of certificates for the services of Multicert CA are performed by members of Multicert's PKI Working Groups.

3.2.1.5 Advanced Certificate (NC)

For advanced certificates issued in the domain of Multicert CA, it is not compulsory that the record is done in person, this is, the initial validation of the applicant identity doesn't have to be done "face-to-face" (or equivalent method). However, along with the request of issuance of advanced certificate, Multicert requests the sending of documentation with which the data in the form is validated, namely the titleholder's data, and the Responsible Entity which requires the certificate. The signatures in the form are verified comparatively to the requested copies of identification documents.

These procedures comply with TS EN 319 411-3document.

3.3 Identification and authentication for key renewal requests

The identification and authentication for the renewal of certificates is performed adopting the procedures for the initial authentication and identification. (cf. section 3.2).

3.3.1 Identification and authentication for routine key renewal

There is no routine key renewal. The renewal of certificates adopts the procedures for the initial authentication and identification, in which new key pairs are generated.

3.3.2 Identification and authentication for key renewal, after revocation

After revocation of the certificate, the generation of a new key pair and corresponding issuance of certificate follow the procedures for initial authentication and identification.

3.4 Identification and authentication for revocation request

The Revocation process for certificates issued by Multicert CA, always begin with the SUSPENSION, allowing that the revocation request is duly validated.

3.4.1 Who can request the certificate revocation

The revocation request can be performed by one of the following:

- The titeholder or the representative person,
- The entity which required the certificate,
- Multicert, every time that this has information that the data on the certificate are not true, or it is not in hold of its titleholder.

After receiving the certificate's revocation request, the documentation received is validated. The identification and authentication of the parts involved in the revocation process request is done through verification, by similarity, of the signatures included in the form and the requested copies of the identification documents.

3.4.2 Procedure for a Revocation Request

The Revocation Request can be performed in two ways:

- Online, through the service made available for this purpose, through service provided for that purpose, one of the following addresses listed below. the certificate moving to the status of SUSPENDED and only after the documentation inherent to the request is received and duly validated, can Multicert change the status to REVOKED:
    - Suspension Interface of certificates issued until 26/05/2015 (certificates with reference MAE or MRA): https://pki.multicert.com/suspensao;
    - Suspension Interface of certificates issued before 27/05/2015 (certificates with refence MTC): https://www.multicert.com/suspensao.
- Or, sending the Revocation Request Form, made available by Multicert on its *site*, directly to Multicert, duly completed and accompanied by the necessary documentation to that effect.

4 Certificate life-cycle operational requirements

4.1 Certificate application

The request of issuance of any certificate to Multicert CA begins with the filling of a form which is appropriate to the desired certificate. The forms for each type of certificate are available on the Multicert Online Store. For each type of certificate the necessary information and the process to be followed are indicated.

4.2 Certificate application processing

4.2.1 Identification and Authentication of the Certification Application

Multicert, as soon as receives the form requesting the issuance of certificate and all requested information needed for the certificate issuance approval, validates all available information in order to verify the authenticity of the data (cf. section 3.2).

4.2.2 Approval or Rejection of the Certificate Application

Multicert only accepts the certificate request for issuance if all the data contained in the request is authentic, in this case the approval of the certificate application takes place.

In the event that the information contained herein is not true or absent Multicert rejects the certificate application and informs the entity responsible for the request.

4.2.3 Time to process Certificate Applications

Multicert has SLAs for certificate issuance, whose information is available on the Online Store, for each of the profiles. However, the issuance of certificates and the time that goes between the certificate application and the delivery of the certificate depend mainly on the readiness of the information provided and its truthfulness.

4.3 Certificate issuance

Multicert CA's certificates are issued automatically through Multicert PKI platform, after the certificate request registered and approved.

The key pair is generated in HSM, the request of certificate issuance is sent to Multicert CA, which will issue the certificate.

4.3.1 CA Actions during the Certificate Issuance

Any certificate issued in the Multicert PKI has to be approved. This approval depends on the type of certificate and the Certification Authority envolved. For end-user certificates approval, the Registry Administration Working Group is responsible for managing and processing certificate requests.

4.3.2 Qualified Digital Certificates Issuance

4.3.2.1 Electronic Signature and Electronic Seal

In the case of Qualified Certificates of Signature and Electronic Seal, the certificate will be stored in a secure criptografic device, which depending on the option chosen, may be SmartCard (chip card), an USB token or a HSM.

4.3.2.2 Certificados para autenticação de sítios Web

For Webserver Certificates issuance, a certificate request is generated by the client and sent to Multicert. The corresponding certificate (CER) is then issued and made available by Multicert to the client by e-mail.

4.3.3 Advanced Certificates Issuance

The Advanced Certificates can be made available in a safe storing device, in the same way as the qualified digital certificates, and also through download or in a CD (depending on the option chosen).

4.3.4 Virtual TPA Certificates Issuance

Multicert CA will issue the certificate (P12) and will be made available in a CD.

4.3.5 Application Certificates Issuance

To issue the Application Certificates, a certificate request is generated by the client, who sends it to Multicert, and the certificate is then issued, based on the request, by Multicert CA, which will be made available through Download or CD.

4.3.6 Notification of Certification Issuance

Any certificate holder is automatically notified when the certificate is issued.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

For each type of certificate, the corresponding Certificate Policy describes the way of accepting it.

The Qualified Signature certificates are issued suspended and it is the responsibility of the titleholder to activate them through a set of information exchange between himself and Multicert.

4.4.2 Publication of the certificate by the CA

Multicert does not publish the certificates it issued, except for its own certificates and their public keys.

4.4.3 Notification of certificate issuance by the CA to other entities

Multicert does not notify other entities about the issuance of certificates except in agreement previously established for the issuance of certificates with its own approval system.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of the private key corresponding to the cerificate's public key, shall be only allowed when the titleholder is in accordance and accepts the general conditions of issuance of a certificate in the time he subscribes it, through the contract supplied by Multicert.

The certificates' titleholders can only use the private key of their certificate to the purpose it was intended (defined in the certificate's "*KeyUsage*" field) and always within legal purposes. Its usage is always the titleholder's responsibility.

4.5.2 Relying party public key and certificate usage

Not Applicable.

4.6 Certificate renewal

The renewal of a certificate is the process in which the issuance of a new certificate uses previous data from the certificate, and there are no changes to the keys or any other information, except the validity period of the certificate.

This practice is treated procedurally as a reference in Multicert's PKI.

4.6.1 Circumstances for renewing a certificate

Nothing to remark.

4.6.2 Who can request the renewal of certificate

Nothing to remark.

4.6.3 Processing the certificate renewal request

Nothing to remark.

4.6.4 Notification of new certificate issuance to subscriber

Nothing to remark.

4.6.5 Procedures for accepting a certificate

Nothing to remark.

4.6.6 Publication of certificate after renewal

Nothing to remark.

4.6.7 Notification of issuance of certificate to other entities

Nothing to remark.

4.7 Certificate renewal with generation of a new key pair

Multicert sustains the renewal of a certificate with generation of a new key pair, being always considered a new issuance.

4.8 Changes in certificates

Changes in certificates is the process through which a certificate is issued for a titleholder (or sponsor), maintaining its corresponding keys and changing only the information on the certificate.

This procedure is not sustained by Multicert CA.

4.8.1 Reasons for changing the certificate

Nothing to remark.

4.8.2 Who can submit a certificate change request

Nothing to remark.

4.8.3 Processing of a certificate change request

Nothing to remark.

4.8.4 Titleholder notification as to the issuance of a changed certificate

Nothing to remark.

4.8.5 Procedures for acceptance of a changed certificate

Nothing to remark.

4.8.6 Publication of the changed certificate

Nothing to remark.

4.8.7 Notification of issuance of a changed certificate to other entities

Nothing to remark.

4.9 Certificate suspension and revocation

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

The certificates which assume the status of SUSPENDED may recover their validity. Certificates which assume the status of REVOKED cannot recover their validity.

A process of revocation of a certificate issued by Multicert CA, begins with its SUSPENSION.

In the case of a Qualified Digital Certificate, this can only maintain the status of SUSPENDED for 3 days, after which the certificate will assume one of the following status:

- Revoked, if the Revocation Request For mis received and validated along with the required documentation, or
- ACTIVE otherwise.

4.9.1 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 (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.

4.9.2 Who Can Request Revocation

It is described in section 3.4, who can ask for the revocation of a certificate and how to do it.

4.9.3 Procedure for Revocation Request

It is described in section 3.4, who can ask for the revocation of a certificate and how to do it.

4.9.4 Revocation Request Grace Period

The Certificate Revocation Process begins with a certificate suspension. The holder / certificate holder has 3 working days to activate the certificate, otherwise it will be immediately revoked.

4.9.5 Time within which the CA Must Process de Revocation Request

Multicert guarantees the publication of the new status of the certificate 24 hours after the request for revocation whenever it proves to be reliable.

4.9.6 CRL Issuance Frequency

Multicert Certification Authorities for end-users issues crl's every 7 days and Delta CRLs are issued every 24 hours.

4.9.7 On-Line Revocation/Status Checking Availability

Multicert has a valid online certificate status validation service with a 99.9% availability service. The OCSP service provides real-time validation of certificate status.

4.10 Services on the status of a certificate

4.10.1 Operational Characteristics

The status of the issued certificates is openly available through CRLs, Delta-CRLs and OCSP service.

4.10.2 Availability of the service

The service on the status of the certificate is available 24 hours a day, 7 days a week.

4.10.3 Optional characteristics

Nothing to remark.

4.11 End of the subscription

The end of the operability of a certificate happens when one of the following circumstances is verified:

a) Revocation of the certificate;

b) Expiration of the certificate's validity period.

4.12 Key retention and recovery (*Key escrow*)

Multicert CA only retains its private key.

4.12.1 Policies and practices of recovering keys

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

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

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

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

4.12.2 Policies and practices for encapsulating and recovery of the session keys

Nothing to remark.

5 Physical safety, management, and operating measures

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

5.1 Physical safety measures

5.1.1 Physical location and construction type

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

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

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

a) Masonry, concrete or brick walls;

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

c) Nonexistence of windows;

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

Additionally, the following security conditions are ensured in Multicert CA environment:

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

5.1.2 Physical access to the location

Multicert CA systems are protected by, at least, 4 hierarchical physical security levels (the building itself, high security block, high security area, high security room), ensuring that the access to a higher security level is only possible when one has previously reached the necessary privileges for the immediately prior level.

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

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

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

5.1.3 Energy and air conditioning

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

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

5.1.4 Exposure to water

High security zones have the proper mechanisms installed (flood detectors) to minimize the flood impact in the systems of Multicert CA.

5.1.5 Fire prevention and protection

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

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

5.1.6 Safeguarding storage support

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

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

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

5.1.7 Elimination of waste

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

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

5.1.8 External installations (alternative) for backup recovery

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

5.2 Process safety measures

The activity of a Certifying Entity depends on the coordinated and complementary intervention of an extensive human resource cast, namely because:

- Given the inherent security requirements to the operation of a CA, it is vital to ensure a proper responsibility segregation, which minimizes the individual importance of each participant;
- It is necessary to ensure that the CA can only be subject to *denial-of-service* type of attacks by means of collusion by a significant number of participants.

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

5.2.1 Working Groups

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

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

Entries in the "Production Environment" are not allowed without the minimum presence of two elements, belonging to distinct Working Groups (with the exception of the Custody Working Group that is not allowed to access this environment).

As an additional security measure, Multicert considers relevant, but not mandatory, the presence in all interventions of an Audit element.

5.2.1.1 Setup Working Group

It is responsible for the initial setup and base configuration (hardware and software) of the CA, until its initialization. This group must have a minimum of 1 (one) member.

The group duties are:

- to install, interconnect and configure the CA's *hardware*;
- to install and configure the CA's base *software*;
- to configure the required initial passwords[8], which will be then changed by the Authentication Working Group;
- to prepare statements about:
    - Initial passwords;
    - Identification of the Setup Working Group members;
    - *Hash* of the CD(s) used in the setup;
    - List of all artefacts (unequivocally identified) indispensable to the CA's initial setup and operation.

5.2.1.2 Operation Working Group

It is responsible for performing the routine tasks essential to the proper functioning and correct operation of the CA.

[8] BIOS, SO administrator account, etc

This group's responsibilities are:

- Management of the "Production Environment" and of the "Operation Environment";
- To perform the CE's routine tasks, including backup copy operations of its systems,
- To perform the CE's system monitoring tasks;
- To monitor, report and quantify all *software* and *hardware* incidents and malfunctions, triggering the appropriate correction processes;
- To request the approval of the forms resulting from the ceremonies to the Management Working Group for storage in the information environment.
- To assume the role of "Registration Administrator" To assume the role of "System Administrator" To assume the role of "System Operator"

5.2.1.3 Authentication Working Group

It is responsible for ensuring the management, safeguard and availability (in the foreseen situations) of the (non-personal) passwords and authorization *tokens*. Please note that, in order to ensure high security levels and business continuity, this group is subdivided into 2 (two) subgroups, consisting of at least 3 (three) members each, who should alternate in the participation in the CE's ceremonies. Each member can exclusively belong to a unique subgroup.

None of the members from this group is authorized to enter in the "Operation Environment" without the presence of a member of the "Audit Working Group".

This group's responsibilities are:

- To define all CA policies and ensure that they are updated and adapted to its reality;
- To ensure that the CA CPs are supported by the CA CPS;
- To ensure that all documents relevant and directly or indirectly related with the CA operation are stored in the Information Environment;
- Management of the "Authentication Environment";
- Management of all non-personal passwords;
- To keep an updated inventory of all the authentication *tokens* used in the "Production environment", and when the *tokens* are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the "Authentication Environment";
- To keep an updated inventory of all the passwords[9] used in the "Production environment", and when the passwords are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the "Authentication Environment";
- To ensure that each member of the remaining groups do not hold any more authentication *tokens* than what is strictly necessary to perform the entrusted responsibilities;
- To ensure that each member of the remaining groups do not hold any more authentication passwords than what is strictly necessary to perform the entrusted responsibilities;
- To register the return of the authentication *tokens* used by the members of the remaining groups;

[9] Registando o seu valor

- To register changes in the authentication passwords used by the members of the remaining groups;
- To register the loss of authentication *tokens*, properly describing the originating situation;
- To always register when an authentication password is compromised, properly describing the originating situation;
- To assess the business risks deriving from the loss of a *token* or the compromising of an authentication password;
- To take active measures not to compromise each Production Environment deriving from the loss of a *token*, or the compromising of any authentication password;
- To assess the documentation replication requests.
- To assume the *Security Administrator* role.

5.2.1.4 Audit Working Group

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

This group's responsibilities are:

- To audit the performance and to confirm the accuracy of the CA's processes and ceremonies;
- To register all sensitive operations;
- To investigate procedural fraud suspects;
- To regularly verify the functionality of the security controls (alarm devices, access control devices, fire sensors, etc.) present in the several environments;
- To register the results of all the actions they perform;
- To assume the role of "System Auditor",
- To validate that all used resources are secure;
- To verify periodically the integrity of the Custody Environments, ensuring that the respective artefacts are found there[10] and are duly identified;
- To verify periodically the records/logs of the CA;

5.2.1.5 Custody Working Group

It is responsible for the custody of some sensitive artefacts (authentication *tokens*, etc.), which may be collected by the members of the other Working Groups by the fulfilment of certain conditions[11]. Please note that, in order to improve the security levels, the business operability and continuity of the CA, there may exist several instances of this group, each in charge of the custody of a distinct set of artefacts. This group shall make use of the several safe environments available for the safekeeping of this type of items. This group shall have at least 2 (two) members.

This group's responsibilities are:

- Management of the "Custody Environment";

[10] In case any of it is borrowed, the Audit Working Group has to verify if there is a record of its delivery and contact the involved members in order to confirm that they have it in their power.
[11] Defined for each artefact in its custody.

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

5.2.1.6 Registration Operation Working Group

It is responsible for ensuring the issuance, renewal, suspension and revocation of certificates.

This group's duties are:

- To assume the "Registration Administrator" role;To validate the documentation to be delivered by the titleholder for the issuance/revocation of certificates;
- To issue certificates when the procedure is not automatised;
- To revoke/suspend certificates in case this procedure is not automatised.

5.2.1.7 Monitoring and Control Working Group

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

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

This group's responsibilities are:

- To consolidate and analyse the monitoring of the resources used in Multicert CA;
- To ensure the continuous improvement to the "Incident management process" and related operational management;
- To collaborate with the Audit Working Group with the purpose of promoting continuous improvement actions;
- To monitor the operation of the existing alarms;
- To make production passages required by pre-production;
- To monitor events, manage alarms and classify incidents;
- To define, support the implementation and continuous improvement of incident response procedures;
- To make production passages required by pre-production.

5.2.1.8 Management Working Group

It is the decision-making body of Multicert CA, ad its members are directly appointed and / or destituted by Multicert's Board of Directors.

The mission of the Management Working Group is mainly based on decision-making which is important and critical to the proper operation of Multicert CA, enhancing the revision and approval of all documents and policies of the CA. The Management Working Group is also responsible for naming and/or destituting members of the other Working Groups and the safekeeping of some sensitive artefacts (authentication *tokens*, etc.). This group shall have at least 4 (four) members.

This group's responsibilities are:

- Management of the "Management Environment";
- To review and approve the policies proposed by the Authentication Working Group;
- To advertise new policies to the other members of the groups;
- To name the members for the remaining Working Groups;
- To make the identification of all the individuals belonging to the different Working Groups available in one or more access points, easily accessible by authorized individuals.
- To make critical decisions about the CA operation;
- To review and approve all the forms resulting from the performed ceremonies and all the documents related to the CA operation.

5.2.2 Number of persons demanded per task

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

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

5.2.3 Functions that require separation of responsibilities

The following matrix defines the incompatibilities (marked with ✘) between belonging to the group/subgroup identified in the columns and belonging to the group/subgroup identified in the rows, under the scope of this CA:

If belonging to the Group / Subgroup ...	**May belong to the Group / Subgroup ... ?**	**Instalation**	**Operation**	**Authentication**	**Registration Operation**	**Audit**	**Custody**	**Management**	**Monitoring and Control**
Instalation						✘	✘	✘	
Operation				✘	✘	✘	✘	✘	
Authentication			✘			✘	✘	✘	
Registration Operation			✘			✘	✘	✘	✘

If belonging to the Group / Subgroup ...	May belong to the Group / Subgroup ... ?	Instalation	Operation	Authentication	Registration Operation	Audit	Custody	Management	Monitoring and Control
Audit		✘	✘	✘	✘		✘	✘	✘
Custody		✘	✘	✘	✘	✘		✘	✘
Management		✘	✘	✘	✘	✘	✘		✘
Monitoring and Control					✘	✘	✘	✘	

5.3 Personal Safety Measures

The hiring of staff who perform trust functions in the Working Groups is only possible if the following requirements are fulfilled:

- Being formally appointed to the function;
- Having proper training for the function;
- Prove his/her identity through documentation issued by reliable sources;
- Prove that he/she doesn't have criminal record;
- Present proof of the qualifications and experience demanded by the entity or group which formally appointed him/her;
- Ensure (formally) confidentiality (unless expressly authorized by the legal representatives of the entity that holds the CA) regarding any information about the CA, its operation, its environments and human resources at its service and about the titleholders of the digital certificates issued by it;
- Compromise (formally) to perform the functions for which he/she was appointed and not assume responsibilities which may lead to ethical or deontological problems to their performance. In that sense it is necessary to declare not only knowing the terms and conditions for the performance of the respective functions, as well as the capacity and availability to do them.

5.3.1 Requirements regarding the qualifications, experience, background, and accreditation

The admission of new members in the Working Groups is only possible if they present proof of the required knowledge, qualifications and experience to perform the tasks of the Working Groups.

5.3.2 Background check procedure

Background check results from the accreditation process of individuals nominated to hold positions in any one of the trust functions. The background check[12] includes:

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

5.3.3 Training and experience requirements

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

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

a) Digital certification and Public Key Infrastructures;

b) General concepts on information security;

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

d) Operation of *software* and/or *hardware* used in the CE;

e) Certificate Policy and Certification Practices Statement;

f) Recovery from disasters;

g) Procedures for the continuation of the activity, and

h) Basic legal aspects regarding the certification services.

5.3.4 Frequency and requirements for recycling actions

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

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

5.3.5 Frequency and sequence of function rotation

Nothing to remark.

5.3.6 Sanctions for unauthorised actions

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

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

Sanctions are applied according to the work rules, national laws and national security laws, to all the individuals who perform unauthorized actions or make unauthorized use of the systems.

5.3.7 Requirements for service providers

Independent consultants or service providers have permission to access the high security zone as long as they are escorted and directly supervised by Working Group members, and after taking notice and accepting the Confidentiality Privacy Statement for External Contributor or Guest [13], existing for this purpose.

5.3.8 Documentation provided to personnel

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

5.4 Security audit procedures

5.4.1 Type of registered events

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

- Request, issuance, renewal, reissuance and revocation of certificates;
- CRL publication;
- Events related with safety issues, including:
    - Access attempts (successful or not) to sensitive CE's resources;
    - Operations performed by members of the Working Groups,
    - Physical safety devices of entry/exit of several levels of security.

The entries in the records include the following information:

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

5.4.2 Frequency of the records audit

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

5.4.3 Retaining period for auditing records

The records are maintained for at least 2 (two) months after processing, and then stored under the terms described in section 5.5.

[13] Multicert_PJ.CA3_28_0001_en - Privacy Statement for External Contributor or Guest

5.4.4 Protection of the auditing records

The records are exclusively analysed by authorized members belonging to the Working Groups.

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

5.4.5 Record backup copy procedures

Backup copies of records are regularly created in high capacity storage systems.

5.4.6 Record collection system (Internal / External)

The records are simultaneously collected internal and externally to the CE's system.

5.4.7 Notification of agents causing events

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

5.4.8 Assessment of vulnerabilities

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

5.5 Record storage

5.5.1 Type of data stored

All auditable data are stored (as indicated in section 5.4.1), as well as information about the certificate requests and support documentation to the life cycle of the different operations.

5.5.2 Period for retaining stored files

The data subject to archiving is retained for a period of time of not less than 7 years.

5.5.3 Archive protection

The archive:

- Is protected so that only authorised members of the Working Groups may consult and access to its content,
- Is protected against any change or attempt to remove it,
- Is protected against the deterioration of the media where it is stored, through the regular migration to a new media,
- Is protected against obsolescence of the *hardware*, operating systems and other *software*, through the conservation of the *hardware*, operating systems and other *software* which then

make part of the archive itself, in order to allow the access and use of the stored records in a timeless manner, and

- Is stored in a safe manner in external environments.

5.5.4 Procedures for the backup copies of the archive

Backup copies of the archives are done in an incremental or total manner and stored in appropriate devices.

5.5.5 Requirements for chronological validation of the records

Some entries in the archives contain date and time information based on a safe time source.

5.5.6 Stored data collection system (Internal / External)

The stored data collection systems are internal.

5.5.7 Procedures for recovering and checking stored information

Only authorised members of the Working Groups have access to the archives, checking their integrity through its restoration.

5.6 Key renewal

Nothing to remark.

5.7 Recovery in case of disaster or compromise

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

5.7.1 Procedures in case of incidents or compromise

The backup copies of the CE's private keys (created and stored according to section 6.2.4) and of the archived records (section 5.5.1) are stored in external safe environments and available in case of disaster or compromise.

5.7.2 Corruption of the computer resources, *software* and/or data

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

If it is confirmed that computer resources, *software* and/or data are corrupted, appropriate measures shall be taken to respond to the incident. The response to the incident shall include the recovery of the corrupted equipment/data, using similar equipment and/or recovering stored backup copies and records. Until the safe conditions are restored, Multicert CA shall suspend its services and notify the accreditation authority.

5.7.3 Procedures in case the entity's private key is compromised

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 certificates issued in the trust hierarchy "branch" from Multicert CA;
- Notification of the Accreditation Authority and all 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.

5.7.4 Capacity to continue the activity in case of disaster

Multicert has the computing resources, *software*, backup copies and records stored in its safe secondary facilities, necessary to restore or recover essential operations (certificate issuing and revocation with the publication of the revocation information) after a natural disaster or other.

5.8 Procedures in case of extinction of the CA or RA

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

a) Inform the Accreditation Authority;

b) Inform all certificate titleholders;

c) Revoke all issued certificates;

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

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

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

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

6 TECHNICAL SAFETY MEASURES

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

6.1 Generation and installation of the key pair

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

6.1.1 Generation of the key pair

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

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

The private key for the certificates issued to a natural or collective person are generated by Multicert CA using cryptographic *hardware* compliant with FIPS 140-2 level 3 and/or *Common Criteria* EAL 4+ requirements.

The operation of Multicert CA is performed in *offline* mode.

6.1.2 Delivery of the private key to the titleholder

The delivery of the private key associated to the certificates of a natural or collective person is performed in SSCD cryptographic device (*Secure Signature-Creation Device*).

6.1.3 Delivery of the public key to the certificate issuer

The public key is delivered to Multicert CA, according to the procedures mentioned in section 4.4.

6.1.4 Delivery of the CA's public key to the trusting parties

The public key from Multicert CA shall be made available through the certificate from Multicert CA, according to section 2.2.

6.1.5 Key size

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

- 4096 bits RSA for the key from Multicert CA,
- 2048 *bits* RSA for the keys associated to the remaining certificates issued by Multicert CA with signature algorithm sha256RSA.

6.1.6 Generation of the public key parameters and quality check

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

The CA's keys are generated based on the use of random/pseudo random processes described on ANSI X9.17 (Annex C), according to the stipulated in PKCS#11.

6.1.7 Key purposes (field "*key usage*" X.509 v3)

According to section 7.1.

6.2 Protection of the private key and features of the cryptographic module

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

6.2.1 Safety standards and measures of the cryptographic module

For the generation of the key pairs from Multicert CA, as well as for the storage of the private keys, Multicert uses a cryptographic module in *hardware*, which complies with the following standards:

- Physical Security
  - *Common Criteria* EAL 4+ and/or
  - FIPS 140-2, level 3
- Regulatory Certifications
  - U/L 1950 & CSA C22.2 *safety compliant*
  - FCC Part 15 – Class B
  - ISO – 9002 Certification
- Papers
  - Two factor authentication
- API support
  - PKCS#11
  - Microsoft CryptoAPI

- Java JCE/JCE CSP
- Open SSL

– Creation of random numbers
  - *ANSI* X9.17 (Annex C)

– Key change and asymmetric key cipher
  - RSA (512-4096 bit), PKCS#1 v1.5, OAEP PKCS#1 v2.0
  - Diffie-Hellman (512-1024 bit)

– Digital Signature
  - RSA (512-4096 bit)
  - DSA (512-1024 bit)
  - PKCS#1 v1.5

– Symmetric key algorythms
  - DES
  - 3DES (double and triple length)
  - RC2
  - RC4
  - RC5
  - AST
  - CAST-3
  - CAST-128

– Hash Algorythms
  - SHA-1
  - SHA-256
  - MD-2
  - MD-5

– Message Authentication Codes (MAC)
  - HMAC-MD5
  - HMAC-SHA-1
  - SSL3-MD5-MAC
  - SSL3-SHA-1-MAC

6.2.2 Multi-personnel control (*n* of *m*) for the private key

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

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

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

activate the private key from Multicert CA stored in the *hardware* cryptographic module. Two parts (n) are necessary for the activation of the private key form Multicert CA.

6.2.3 Retention of the private key (key escrow)

Retention of Multicert CA's private key is explained in detail in section 4.12.

6.2.4 Backup copy of the private key

The private key from Multicert CA has at least one backup copy with the same security level as the original key, according to section 4.12.

6.2.5 Storage of the private key

The private keys from Multicert CA, subject to backup copies, are stored as identified in section 4.12.

6.2.6 Transfer of private key to/from the cryptographic module

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

Even if a backup copy of the private keys from Multicert CA is made to another cryptographic *token*, that copy is done directly, *hardware* to *hardware*, thus ensuring the transport of the keys between modules in an enciphered transmission.

6.2.7 Storage of the private key in the cryptographic module

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

6.2.8 Process for activating the private key

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

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

6.2.9 Process for deactivating the private key

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

To deactivate Multicert CA's private keys it is necessary, at least, the intervention of four elements from the Working Group. Once deactivated, this will remain inactive until the activation process takes place.

6.2.10 Process for destroying the private key

The private keys from Multicert CA (including backup copies) are erased/destroyed in a procedure duly identified and audited, as soon as their expiry date (or if they are revoked before that period).

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

6.2.11 Assessment/level of the cryptographic module

Described in section 6.2.1.

6.3 Other aspects for managing key pairs

6.3.1 Storage of the public key

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

6.3.2 Validity periods of the certificate and keys

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

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

- the certificate from Multicert CA has a minimum validity of eleven years and four months, being used to sign certificates during its first five years of validity, and is reissued before it reaches a validity of four years and nine months;
- service certificates (except Web Server certificate) have a maximum validity period of five years and two months, being used during their first month of validity and reissued after 4 months of validity;
- the Web Server certificate has a maximum validity period of three years. Effective March 2018, web server certificates will be issued with a maximum valitdaty perior of two years;
- the certificate of natural person has a maximum validity period of five years, except certificates issued Registration Authorities where the validity is for 4 years;
- the certificate of collective person has a maximum validity of three years.

6.4 Activation data

6.4.1 Generation and installation of activation data

The activation data necessary for using the private key from Multicert CA are divided in several parts (stored in PED keys – small digital identification *tokens*, with physical USB pen format, identifying

different access roles to HSM), and are at the responsibility of the different members of the Working Group. The different parts are generated according to what was defined in the process/ceremony for the key generation, and obey to the requirements defined by standard FIPS 140-2 level 3.

6.4.2 Protection of activation data

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

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

6.4.3 Other aspects from activation data

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

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

6.5 Computer safety measures

6.5.1 Specific technical requirements

The access to the servers from Multicert CA is restrict to the members of the Working Groups with a valid reason for that access. Multicert CA works *online*, and the certificate issuance request is done from the System for Managing the Certificate Life-cycle (SGCVC) and/or the operation console.

Multicert CA and SGCVC have border protection devices, namely a *firewall* system, and comply with the necessary requirements for identification, authentication, access control, administration, audit, reuse, service responsibility and recovery, and information exchange.

6.5.2 Security assessment/level

The various systems and products used by Multicert CA are reliable and protected against changes.

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

6.6 Lifecycle of technical safety measures

6.6.1 System development measures

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

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

6.6.2 Safety management measures

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

6.6.3 Lifecycle of safety measures

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

6.7 Network safety measures

Multicert CA has border protection devices, namely a *firewall* system, and comply with the necessary requirements for identification, authentication, access control, administration, audit, reuse, service responsibility and recovery, and information exchange.

6.8 Chronological validation (Timestamping)

Certificates, CRLs and other entries in the database always have information about the date and hour of that entry. All these entries are digitally signed by a certificate issued for that purpose.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 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 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 titleholder.

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 any type of storage units.[7]

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 zero or more additional certificates from CAs signed by other CAs. [7]

The profile of the certificates issued by Multicert CA is compliant with:

- ITU.T recommendation X. 509[14];
- RFC 5280[7];
- Applicable legislation, national and European;
- Baseline Requirements From CABForum.

The certificate profiles may be consulted in the documents of the Certificate Policies associated to this CPS, according to the table in section 3.1.1.

7.2 Certificate revocation list profile

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

The protocol X.509 defines a method of certificate revocation, which involves the periodic issuing, by the CA, of a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by the CA and made freely available in a public repository. Each revoked certificate is identified in the CRL by its serial number. When an application uses a certificate (e.g., for verifying a remote user's digital signature), that application not only verifies

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

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.[7]

.

The CRL profile conforms to:

- ITU.T Recommendation X.509[14];
- RFC 5280[7] and,
- Applicable legislation, national and European.

The CRL profiles may be consulted in the documents of the Certificate Policies associated to this CPS, regarding to Multicert CA (according to the table in section 3.1.1).

7.3 OCSP profile

The profile of the OCSP certificates is compliant with:

- ITU.T recommendation X.509[14],
- RFC 5280[7] and,
- Applicable legislation, national and European.

The OCSP certificate profiles may be consulted in the documents of the OCSP Validation Certificate Policies associated to Multicert PKI, according to the table in section 3.1.1.

8 COMPLIANCE AUDIT AND ASSESSMENTS

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

Besides the compliance audits, Multicert shall perform other inspections and investigations to ensure the compliance from Multicert CA with the national legislation. The execution of these audits, inspections and investigations may be delegated to an external audit entity.

8.1 Frequency or reason for the audit

The compliance audits are performed periodically in annual basis. The CA must prove, through audit and anual safety reports (produced by the conformity assessment body), that the risk assessment was assured, having identified and implemented all necessary measures for the information security.

8.2 Identity and qualifications of the auditor

The auditor is independent from the circle of influence of the CE, with recognised suitability, holding proved experience and qualifications in the field of security of information and information systems, public key infrastructures, acquainted with applications and programs of digital certification and with the performance of safety audits. His/her mission is to audit the CE's infrastructure, in what concerns equipment, human resources, procedures, policies and rules

The National Accreditation Body is responsible for the accreditation of the Conformity Assessment Bodies, which are qualified to carry out the conformity assessments resulting from these evaluations, a Conformity Assessment Report (CAR) is to be made available to the Supervisory Entity, to evaluate the continuity of the trusted services.
The Security Auditor of Multicert CA is described in section 1.3.5.5 of this document.

8.3 Relation between the auditor and the Certifying Entity

The auditor and members of his/her team are independent, not acting partially or discriminatory towards the entity subject to the audit.

There must be ensured that no contractual relationship exists between the auditor and the entity subject to the audit.

The Auditor and the audited party (Certification Authority) shall have no relation, current or foreseen, financial, legal or of any other type which may lead to conflict of interests.

The fulfillment of what is established by the law in force about personal data protection must be noticed by the auditor, in the sense that the auditor may access personal data of the files of the CA's titleholders.

8.4 Scope of the audit

The scope of audits and other assessments include the accordance with the national legislation and this CPS and other rules, procedures and processes (especially the ones related with key management operations, resources, management and operation controls and management of the certificates life-cycle).

8.5 Procedures after an audit with a poor outcome

If from an audit result irregularities, the auditor proceeds as the following:

a) Documents all faults found during the audit;

b) At the end of the audit he/she gathers with the responsible from the entity subject to the audit and presents briefly a report on his/her first views (RPI);

c) Write the final audit report. This report shall be organised in a way that all faults are staggered in descending order of severity;

d) Submits the final audit report to the Accreditation Authority and simultaneously to the responsibles of the entity subject to the audit for appreciation;

e) Bearing in mind the irregularities stated on the report, the entity subject to the audit will send a correction of irregularities report (RCI) to the Accreditation Authority, where the actions, methodology and time needed for correcting the irregularities, shall be described;

f) The Accreditation Authority, after analysing this report takes one of the following three options, according to the level of severity of the irregularities:

    a. Accepts the terms, allowing the activity to be continued until the following inspection;

    b. Allows that the entity remains in activity for a maximum period of 60 days until the correction of irregularities before the revocation;

    c. Proceeds to the immediate revocation of the activity.

8.6 Communication of results

The results shall always be communicated Supervisory Body.

8.7 Self-Audits

A Self Assessment isto performed annualy by internal auditors.

9 OTHER SITUATIONS AND LEGAL MATTERS

This section deals with business aspects and legal matters.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

Nothing to remark.

9.1.3 Fees for access to information on the status of the certificate or revocation

Access to information on the certificate status or revocation (CRL and Delta-CRL), is free and open.

9.1.4 Fees for other services

The fees for the chronological validation and *on-line* OCSP validation services are identified in a formal proposal to be made by Multicert.

9.1.5 Reimbursement policy

Nothing to remark.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other resources

Nothing to remark.

9.2.3 Insurance or guarantee of coverage for users

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

9.3 Confidentiality of the information processed

9.3.1 Scope of information confidentiality

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

a) The private keys from Multicert CA;

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

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

d) Business continuity and recovery plans;

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

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

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

h) The identification of the members of Multicert CA's Working Groups;

i) The location of Multicert CA's environments and its content.

9.3.2 Information outside the scope of information confidentiality

It is considered as information for public access:

a) Certificates Policy;

b) Certification Practices Statement;

c) CRL;

d) Delta-CRL;

e) All information classified as "public" (the information not expressly considered as "public" shall be considered as confidential).

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

9.3.3 Responsability for protecting confidential information

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

9.4 Privacy of personal data

9.4.1 Measures to guarantee privacy

The SGCVC is responsible for implementing the measures ensuring the privacy of personal data, according to the Portuguese legislation.

9.4.2 Private information

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

9.4.3 Information not protected by privacy

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

9.4.4 Responsibility to protect private information

In accordance with the Portuguese legislation.

9.4.5 Notification and consent for the use of private information

In accordance with the Portuguese legislation.

9.4.6 Release of information resulting from legal or administrative proceedings

Nothing to remark.

9.4.7 Other circumstances for revealing information

Nothing to remark.

9.5 Intellectual property rights

All intellectual property rights, including those which refer to issued certificates, CRL,Delta-CRL, OID, CPS and CP, as well as any other document, property of Multicert CA belong to Multicert, S.A..

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

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

9.6 Representations and guarantees

9.6.1 Representation and guarantees of certifying entities

Multicert CA is obliged to:

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

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

c) Protect its private keys;

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

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

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

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

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

i) Store the certificates issued without any changes;

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

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

l) Revoke the certificates under the terms of section "Certificate Suspension and Revocation" of this document and publish the revoked certificates on the CRL in the repository from Multicert CA, with the frequency stipulated in section 2.3;

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

n) Make available, since dully justified the access request, to the previous versions of its CPS as well as the Certificate Policies;

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

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

q) Operate in accordance with the applicable legislation;

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

s) Guarantee the availability of the CRL in accordance with the dispositions in section 0,

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

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

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

w) Make the certificates from Multicert CA available.

9.6.2 Representation and guarantees of the Registration Entities

Registration Authorities are obliged to:

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

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

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

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

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

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

g) Store the certificates issued without any changes;

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

i) Revoke the certificates under the terms of section "Certificate Suspension and Revocation" of this document and publish the revoked certificates on the CRL in the repository from Multicert CA, with the frequency stipulated in section 2.3;

j) Collaborate with the audits performed by the Accreditation Nacional Body,

k) Operate in accordance with the Regulation 910/2014

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

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

n) Maintain all information and documentation relative to a recognised certificate at each moment and for seven years from issuance.

9.6.3 Representation and guarantees of the titleholders

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

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

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

c) Immediately request that a certificate be revoked in the case of having knowledge or suspicion that the private key corresponding to the public key contained in the certificate has been compromised, according to section 0;

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

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

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

9.6.4 Representation and guarantees of the trusting parties

It is the obligation of the parties that are entrusted with the certificates issued by Multicert CA to:

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

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

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

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

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

f) Notify any occurrence or anomalous situation related to the certificate that may be considered the cause of its revocation.

9.6.5 Representation and guarantees of other participants

Nothing to remark.

9.7 Renouncing guarantees

Multicert CA refuses all service guarantees that are not bound by the obligations set forth in this CPS.

9.8 Limitation to obligations

Multicert CA:

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

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

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

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

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

f) shall not answer if the electronically signed documents' addressee doesn't comprove them and takes into account the restrictions that are stated in the certificate concerning its possible usage, and

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

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

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

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

9.9 Indemnities

In accordance with the legislation in force.

9.10 Termination and cessation of the activity

9.10.1 Termination

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

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

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

9.10.2 CPS substitution and revocation

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

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

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

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

When the CPS is revoked, it shall be removed from the public repository; however it is guaranteed that it will be kept for 7 years.

9.10.3 Consequences of the cessation of activity

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

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

9.11 Individual notification and communication to the participants

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

9.12 Changes

9.12.1 Change procedures

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

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

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

9.12.2 Notification period and mechanism

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

9.12.3 Reasons to change OID

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

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

In case the Authentication Working Group finds the changes to the specification might affect the acceptability of the certificates to specific purposes, it shall take place an increase to the higher version number of the document and the lowest number shall be placed to zero. The last two numbers of the Object Identifier (OID) that represent it shall also be changed. This type of changes shall be communicated to the certificate users in accordance with that set forth in point 9.12.2.

9.13 Dispositions for solving disputes

All complaints between users and Multicert CA shall be communicated by the dispute party to the Accreditation Authority, for the purpose of trying to solve it between the same parties.

To solve any conflict that may arise regarding this CPS, the parties, renouncing to any other courts that may correspond to it, submit themselves to the Administrative Litigation Jurisdiction.

9.14 Applicable legislation

The following specific legislation is applicable to the activities of the Certifying Entities:

a) REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

b) CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.4.

c) CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;

d) CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;

e) ETSI EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

f) ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

g) ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part. 2: Requirements for Trust Service providers issuing EU qualified certificates;

h) ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

i) ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

j) ETSI EN 319 412-3 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

k) ETSI EN 319 412-4 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;

l) ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;

m) ETSI EN 319 421 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;

n) ETSI EN 319 422 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;

o) .

9.15 Compliance with the legislation in force

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

It is the responsibility of the Accreditation Authority to ensure the compliance of the applicable legislation listed in section 9.14.

9.16 Various provisions

9.16.1 Complete agreement

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

9.16.2 Independence

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

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

9.16.3 Severity

Nothing to remark.

9.16.4 Proceedings (lawyer fees and giving up rights)

Nothing to remark.

9.16.5 Force Majeure

Nothing to remark.

9.17 Other provisions

Nothing to remark.

Conclusion

This document defines the procedures and practices used by Multicert Certification Authority 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 informations and electronic documents, ensuring its authorship, integrity and non-repudiation, and ensuring the confidentiality of the transactions or information.

Aprovação